



比特币文凭

迈向比特币时代的金融教育



网址

<https://hcm.capital>

电子邮箱

contact@hcm.capital

X (推特) 账号

@HCM_Capital

比特币文凭

迈向比特币时代的金融教育



学习指南
中文版 | 2025

如您支持本书，
可扫码捐赠



bc1q5es60qpa7gpkp0k32x14zefkj43kd9zjkzd54sgmv3yxr34dw8dqm9pzsd

Mi Primer Bitcoin (My First Bitcoin):

一基于萨尔瓦多的公益性组织，主要做对比特币教育的推广，
是本书《Bitcoin Diploma》的西班牙文及英文版本；

HCM 协助将其编辑和翻译成此中文版本《比特币文凭》。

本作品依据**知识共享署名-相同方式共享4.0国际许可协议(CC BY-SA 4.0)**授权使用。



序言

比特币：一种理想、技术和实践的载体

朱嘉明

经济学家/博士

非营利性非政府组织 Mi Primer Bitcoin / My First Bitcoin (MPB/MFB)(译为“我的第一枚比特币”)是一个充满激情，将比特币视为理想、技术和实践的载体的团队，其核心价值理念是批判性思维、个人责任感和自我主权，构建一个独立、公正、社区主导的新世界。

从2022年开始，MPB以萨尔瓦多作为基地，以全球为目标，通过开源的《比特币文凭》(Bitcoin Diploma)教材，将比特币作为大规模赋权的工具，不断扩大拥有比特币文凭的年轻人群体，打造一台势不可挡的机器，构建全球去中心化的节点网络，为不同利益创造共同旗帜，最终形成一场取代现有秩序的全新的革命。

因为MPB，人们需要重新面对2009年比特币问世的初衷：通过基于区块链技术和算力工具支持的比特币，以结束以国家权力为基础的法币体系垄断货币形态，进而控制财富、资产和资本的历史。在过去的16年间，比特币展现了极为复杂的历史。一方面，支持比特币的技术体系和维系比特币社区运行模式，都得到了验证，形成了以比特币为核心的加密货币生态；另一方面，因为传统资本机构的涌入，比特币的市值和交易规模持续上涨，比特币已经演变为不断膨胀的新型资产类别，与法币挂钩的稳定币参与投资组合。

进入2024年年末，比特币价格一度超过10万美元，比特币交易所交易基金的资金流入持续上升。甚至出现这样的预言：在2020年代后期，比特币市值将超过黄金市值。其重要推动力是包括：比特币代表的加密货币的有限供给量，加密货币和加密资产的无国界特性，世界超过一半的国家和地区承认加密资产的合法性，世界级大公司购入加密货币，以及美国提出了战略比特币储备(Strategic Bitcoin Reserve, SBR)。

但是，非常遗憾的现实是，以比特币代表的加密数字货币在传统资本和金融力量的渗透和影响下，已经与其初衷渐行渐远，正在“异化”成为所谓的“数字黄金”，成为一种资本新游戏。在这样的资本新游戏中，不再可能遵守去中心化原则，必然排斥民众参与。

现在，比特币和其他加密货币正在面临历史的关键时刻：或者回归初衷，成为货币非国家化的一种实验，一种民众的获得生存权利，实现基本收入和财富再分配的工具；或者沦为传统资本和新资本的工具，纳入全球金融体系，加剧数字经济时代的贫富差别。

所以，MPB推动的《比特币文凭》开启了在加密数字货币领域的正本清源，告诉民众真实的货币本质和货币历史，特别是法币与通货膨胀、社会不平等和全球债务的关系，以及比特币原理和融入民主生活的方式。最终教育民众：人们需要赋权未来，所以需要控制自己的金钱和选择比特币。

更近一步，不论是历史上的贵金属货币，还是基于1944年的布雷顿森林会议所构建的，之后的自由汇率制度的当代货币体系，都不再适应从传统工业社会到信息、数字和人工智能时代的转型。唯有比特币，以及其他具有生命力的加密数字货币，可以适应信息、数字和人工智能时代。2008年世界金融危机，就本质原因而言，就是世界金融体系严重滞后于已经改变全球产业结构、经济制度和经济机制。这也是比特币诞生的重要历史原因。

通过MPB和他们开源的比特币文凭教材，解开了围绕比特币的一个历史性博弈：MPB成为比特币初衷、价值观的代表，与社区和民众结合的一方，而以比特币改变为少数人财富工具的大公司、大资本和权力工具为另一方。这将是21世纪第二个25年最为重要的博弈。时间、人民和技术，最终会站在MPB，而不是大公司、大资本和权力一方。因为，只要比特币的知识和实践得以普及，人们会加剧挑战和放弃基于权力垄断的财富工具，拥抱去中心化、透明化、确保个人财富安全和隐私的全新信任体系。

未来路途多么曲折，MPB的努力，正在展现这样的未来真正到来。这样的过程，正是中国唐代诗人刘禹锡所写的那种“千淘万漉虽辛苦，吹尽狂沙始到金”境界。

祝贺在2025年初春之际，《比特币文凭》学习指南的中文版与读者见面。也希望中文读者从中得到启迪和鼓舞。

2025年1月15日 北京

发现比特币，打开新天地

Jerry Beh

《发现比特币》播客主持人

2009年1月3日，中本聪在比特币创世区块留下了这样一句话：“The Times 03/Jan/2009 Chancellor on brink of second bailout for banks”（《泰晤士报》2009年1月3日：财政大臣即将启动对银行的第二轮纾困）。这不仅是比特币的诞生宣言，也是一场针对金融体系现状的深刻反思。从此，比特币作为去中心化的点对点电子现金系统，悄然开启了重塑货币与信任体系的革命。

十六年过去了，比特币已经从一个默默无闻的实验，成长为全球数百万人的信仰与实践。然而，仍然只有少数人以开放的态度去学习、理解并拥抱比特币。其原因之一在于，比特币作为一种颠覆性的创新，挑战了许多传统认知；另一方面，绝大多数关于比特币的内容以外语(特别是英文)为主，语言的壁垒无形中阻碍了更多人接触比特币的机会。

学习比特币不仅仅是技术的探索，更是对我们所处经济环境的清醒认知。在1960年代，我母亲的第一份工作为车衣学徒，领着MYR50的薪资。在那个年代，MYR0.10已经可以买到一碗吃得饱的汤面。如果我的母亲当年将那一个月的薪水存起来，在今天面临的可能是两个残酷的现实：第一，当时的钱币可能已无法作为货币流通；第二，那MYR50在2025年的今天也只够买五碗当年仅需MYR0.10的汤面。这是法币500倍的贬值。在法币的世界，印在纸币上的数目只是一个幻象，我们以为自己拥有的财富数额未变，但其实际的购买力早已被悄悄地掏空。

正因如此，我坚信每个人都需要学习比特币。它不仅是技术与货币的创新，更是通往(经济)自由的桥梁。它给了我们一个选择，不再依赖容易被操控的法币系统，而是通过一个透明且可验证的网络，保护自己的财富免受通货膨胀和集权的侵蚀。

作为一个有幸掌握英文，并怀抱好奇心与开放态度的学习者，我在过去的数年间透过书籍、播客和视频，从多个角度深入理解比特币的本质。我逐渐认识到，比特币的普及不仅仅是一场技术与金钱的革命，更是赋予社会上每个人做自己主人的机会。正是在这种认知下，我萌生了将所学的比特币知识带入中文世界的愿望，于是诞生了《Tom & Jerry发现比特币》播客。这不仅是我推广比特币的尝试，更是为后代留下思想足迹的愿景，让我的孩子们能够通过这些内容，见证我们探索比特币的旅程与思想蜕变。

在这个过程中，我遇到了许多志同道合的比特币支持者。他们来自不同领域，却以各自的方式推动比特币的采用。尤其是与 Jack Lee 及 HCM 团队的交流，更让我深受启发。他们不仅在资金与行动上全力支持比特币的推广，还主动推动了《比特币文凭》这本教材的中文翻译。从这本教材开始，他们正在为中文世界打开一扇比特币教育的大门，帮助更多人打破认知的城墙，建立对比特币的正确理解。

正因为我们处于选择的关键时刻，《比特币文凭》这本书的重要性尤为凸显。这不仅是一本比特币的入门读物，更是一份自救指南。它教会人们如何从法币系统的枷锁中解放自己，如何通过比特币找到(经济)自由的途径。这是每一个渴望自主权的人都需要了解的知识，也是一场个人觉醒与社会转变的教育革命。

学习比特币是一个挑战固有观念的过程，也是一种思想的重生。从凯恩斯经济学派主张政府干预经济到奥地利学派强调自由市场和个人选择的哲学，学习比特币的过程带我们重新审视这个世界，也重新认识内心深处对公平、公正和透明的渴望。

我相信，在不远的未来，越来越多的学校和教育平台会借助这本比特币教科书，帮助更多人系统性地学习比特币的知识与观念。超比特币化的浪潮，不仅是技术的普及，更是每个人拥抱比特币的故事。最终，比特币将引领我们走向一个更自由、更美好的世界。

发现比特币，打开新天地。让我们追随中本聪的起义，去发掘比特币的真正意义。

2025年1月17日 吉隆坡

《比特币文凭》的故事

当一个想法已然成熟，便没有什么能够再阻挡它。

《比特币文凭》的故事始于萨尔瓦多。2022年6月，首批38名公立学校学生完成试点课程并顺利毕业——这是在公立学校体系内推行的全球首例。

实在难以想象，这一切发生仅不到三年。

这个项目自那以来实现了惊人的增长——已有成千上万名学生在全国各地完成课程并毕业。更令人振奋的是，这股增长的力量不仅来自我们自身，而是源于全球各地的比特币教育者。他们积极采纳了这本开源教材，无论是在萨尔瓦多，还是在世界各地，都在推动比特币教育的普及。

萨尔瓦多教育部将其作为本国比特币文凭课程的核心教材，并在2024年，我们与比特币海滩(Bitcoin Beach)合作，培训了400多名公立学校教师，让他们能够在自己的学校教授这门课程。

萨尔瓦多是重中之重，其使命全球。

2023年3月，我们成立了国际比特币教育者节点网络，所有加入的节点都需遵守一系列核心原则：教育必须独立、公正、由社区主导，专注比特币，高质量，并致力于赋能。如今，该网络已实现自我治理，并将课程内容翻译成八种以上语言，在加拿大、美国、墨西哥、危地马拉、洪都拉斯、哥斯达黎加、古巴、多米尼加共和国、海地、哥伦比亚、苏里南、秘鲁、巴西、阿根廷、爱尔兰、英国、葡萄牙、格鲁吉亚、加纳、尼日利亚、乌干达、肯尼亚、赞比亚、津巴布韦、南非、阿富汗、孟加拉国、印度、香港、印尼和澳大利亚等地推广比特币文凭课程。该网络每月都会新增节点，而由于内容是开源的，任何人都可以自由使用，无需获得许可。事实上，可能还有许多人已经自发地在各地推动其进程。

这是一场全球性的、去中心化的运动。

独立、公正、由社区主导的比特币教育将改变世界——而事实上，这一切已经悄然开始了。

为了更美好的世界

Mi Primer Bitcoin (My First Bitcoin) 团队 - 2025年

目录

第1章：为什么我们需要钱？

1.0 引言	01
1.1 认识聪聪	01
活动：关于金钱的五个问题	01
1.2 课堂讨论：为什么我们需要钱？	04

第2章：货币是什么？

2.0 引言	07
活动：课堂讨论——“货币是什么？”	07
2.1 货币的定义	07
2.2 货币的功能	09
2.3 货币的特性	10
2.4 货币的种类	13
2.5 货币心理学：稀缺性、时间偏好与权衡	14
活动：时间偏好	16

第3章：货币的历史

3.0 引言	21
活动：以物易物游戏	21
3.1 从以物易物到现代货币的演变	23
3.1.1 早期货币形式存在的问题	23
3.1.2 硬币和纸币的发展	24
3.1.3 从“稳健货币”到“不稳健货币”的转变	25
3.1.4 从纸币到银行卡	27
3.2 数字货币	28

第4章：什么是法定货币？法定货币由谁控制？

4.0 引言	31
4.1 法定货币简史	31
4.2 法定货币系统	34
4.2.1 法定货币体系	34

4.2.2 部分准备金银行制：由债务驱动的系统	35
活动: 部分准备金银行制	38
4.2.3 谁控制着法定货币系统？他们如何从中受益？	39
4.3 中央银行数字货币：法定货币的未来	41

第5章：问题如何促成解决方案

5.0 问题简介	45
5.1 购买力下降	45
5.1.1 货币通胀及其对购买力的影响	45
活动: 通货膨胀的影响：拍卖活动	46
5.2 全球债务负担与社会不平等	47
5.2.1 对个人的影响——购买力的丧失	47
5.2.2 对社会的影响——财富不平等加剧	52
活动: 法定货币体系的后果	53
5.2.3 全球债务负担	54
5.3 密码朋克与去中心化货币的探索	55
5.3.1 密码朋克	56
5.3.2 集中化与去中心化系统	57
5.3.3 数字货币简史	59

第6章：比特币简介

6.0 中本聪与比特币的诞生	63
6.1 比特币是如何运作的？	65
6.1.1 中本聪共识机制	65
6.1.2 游戏的参与者	67
活动: 在点对点网络中建立共识	69
6.2 作为稳健数字货币的比特币	71
6.2.1 引言	71
6.2.2 比特币的特性	72
活动: 课堂讨论 - 比特币是稳健货币吗？	76
6.2.3 承担个人责任	76

第7章：如何使用比特币

7.0 引言	81
7.1 获取和兑换比特币	81
7.1.1 点对点：线下	81
7.1.2 点对点：线上	82
7.1.3 集中式交易所	82
7.2 比特币钱包简介	83
7.2.1 自托管钱包与托管钱包	83
7.2.2 不同类型的比特币钱包	85
7.2.3 开源与闭源	86
活动：课堂评估比特币钱包	87
7.3 设置移动比特币钱包	87
活动：设置/恢复比特币钱包	87
7.4 接收和发送交易	89
活动：比特币交易实践	91
7.5 比特币储蓄	93
7.6 自己研究——不要相信，去验证	94

第8章：闪电网络：将比特币融入日常生活

8.0 引言	97
活动：观看《比特币闪电网络解析：它是如何运作的》	98
8.1 闪电网络	98
8.2 不同类型的闪电钱包	100
8.2.1 自托管钱包与托管钱包	100
8.2.2 开源与闭源	100
8.3 创建一个比特币闪电钱包	100
8.4 闪电交易的发送和接收	102
活动：闪电钱包接力赛	106
8.5 用比特币购买咖啡和日用品	107
8.5.1 线上：支付插件 - 电子商务	108
8.5.2 线下：寻找本地商家	109
8.5.3 过渡工具：礼品卡与支付卡	110
8.5.4 循环经济与比特币作为交易媒介	110

第9章：从技术层面介绍比特币

9.0 引言	115
活动: 观看《比特币的技术原理详解》	115
9.1 公钥与私钥：通过加密技术实现安全	116
9.1.1 公钥/私钥的加密原理	116
9.1.2 哈希的解释	119
活动: 生成SHA-256哈希值	121
9.2 UTXO模型	122
9.3 比特币节点和矿工	125
9.3.1 什么是比特币节点，我又该如何设置？	125
活动: 观看关于比特币节点的视频	126
9.3.2 什么是比特币矿工，挖矿是如何进行的？	126
9.4 什么是内存池？	132
活动: 内存池	134
9.5 比特币交易如何从开始到完成	135

第10章：为什么选择比特币？

10.0 引言	139
活动: 比特币的未来是什么样的？	139
10.1 什么是中央银行数字货币(CBDCs)，由谁控制？	140
10.2 比特币的哲学	141
活动: 课堂讨论：你是否有权控制自己的金钱？	141
10.3 比特币的优势	142
10.4 赋权未来	143
活动: 课堂讨论：你的观点发生了怎样的变化？	143
附加资源	147
各章关键概念	149
术语表	153

比特币文凭

为期十周的独立、公正、高质量，
以及免费的教育变革之旅

在学习比特币之前，牢牢掌握有关金钱的基础知识、历史渊源，以及当前的金融体系至关重要。理解这些概念能够为我们认识比特币的独特性和颠覆性奠定坚实的基础。通过了解金钱的演变，您将能够更好地理解当前金融体系的潜力和局限性，以及比特币是如何致力于解决这些问题的。如果没有这样的基础，我们可能很难完全理解比特币的意义及其潜在影响。相信学习的过程并保持专注，对这一尖端领域的更深层次理解和欣赏，终将为我们带来丰厚的回报。

第一章

我们为什么 需要货币？

1.0 引言

1.1 认识聪聪

活动: 关于货币的五个问题

1.2 课堂讨论: 我们为什么需要货币?

我们为什么需要货币？

1.0 引言

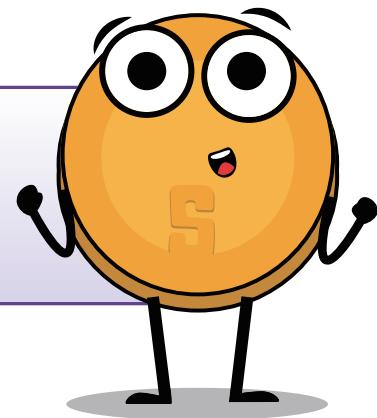
“货币是人类发明的最伟大的自由工具之一。”

弗里德里希·哈耶克

欢迎来到比特币文凭课程。在本章中，我们将探讨一个基本问题：为什么货币在我们的生活中如此重要？我们将研究货币的本质及其各种形式，旨在更深入地了解其意义。我们几乎每天都在使用货币，可我们真的知道自己为什么需要货币吗？货币又究竟是什么？为什么我们的父母和家人要用他们的时间来换取货币？为什么有些人比其他人拥有很多货币？为什么不同国家的货币不一样？为什么我们不能在自己需要的时候创造更多的货币？

1.1 认识聪聪

“嗨！我是聪聪，一个互动助手，我会在比特币文凭课程中为你提供帮助。接下来，我将为你提供资源和有用的建议，帮助你更深入地了解关键概念。”



活动：让我们从回答下面的 5 个问题，并开始本章的学习。

考虑货币的实际用途，如获取食物等必需品和想要的物品。在举例时需尽量具体，兼顾创意和现实。



第一章



我们为什么需要货币？

货币是什么？

我们为什么需要货币？

谁在控制货币？

是什么给了货币“价值”？



第一章



你有什么关于货币的问题？把你的问题写下来并和全班同学分享。

拓展讨论：将你的答案与全班同学进行分享并比较，找出需要货币的最重要的五个理由。确定在班级中有哪些想法是相同的。反思你个人独特的想法（即使它们没有被列入名单，也值得考虑），并记录下这些额外的见解。

1.2 课堂讨论：我们为什么需要货币？

班级分组并完成以下任务。

- ◆ 分享并讨论他们对前四个问题的答案，写下自己最喜欢的答案。
- ◆ 分享他们对最后一个答案，并投票选出学生的问题中最受欢迎的那个，记录结果。
- ◆ 在比特币文凭课程结束时，全班同学重温答案和问题。

现在，你对货币的必要性有了更清晰的理解。在接下来的章节中，我们将继续探讨货币是什么、它是如何随着时间演进的、谁在影响它，以及货币的最新形式。继续参考你在课堂第一天写下的列表，将你的见解与货币的创造、定义和使用的演变联系起来。

第二章

货币是什么?

2.0 引言

活动: 课堂讨论 - “货币是什么?”

2.1 货币的定义

2.2 货币的功能

2.3 货币的特性

2.4 货币的类型

2.5 货币心理学: 稀缺性、时间偏好与权衡

活动: 时间偏好

货币是什么？

2.0 引言

货币可以保障我们能够在将来拥有自己想要的东西。
尽管此刻我们可能无所需求，但货币使满足新需求成为可能。

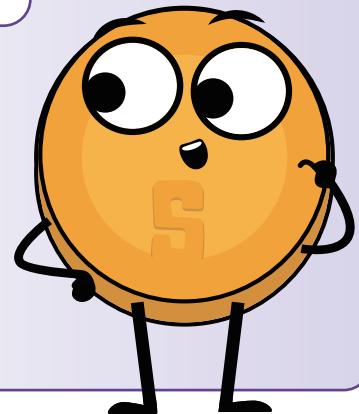
亚里士多德

本章以我们对货币必要性的探索为基础，对核心问题进行探讨：货币是什么？首先，我们将进行小组讨论和活动。

活动：课堂讨论 —— “货币是什么？”

- ✿ 请先不要吃放在你桌上的糖果。
- ✿ 谁愿意用自己的糖果换一张1美元的钞票？
- ✿ 如果现在你还愿意用1美元的大富翁钞票来换你的糖果的话，请继续举手。
- ✿ 为什么愿意，又为什么不愿意？
- ✿ 是什么让一张钞票如此受欢迎，另一张钞票却像垃圾一样？
- ✿ 是什么赋予了货币“价值”？
- ✿ 钱是从哪里来的，由谁来决定该印多少钱？
- ✿ 为什么不印更多的钞票，然后平均分配给每个人？

这两张钞票之间唯一的区别在于，你相信其中一张比另一张更有价值。



2.1 货币的定义

你有没有停下来思考过，货币到底是什么？大多数人都知道该如何使用货币，却很少有人了解它的来源或运作方式。从本质上来说，货币是交换商品和服务的一种方式，它以便于交易的形式代表这些物品的价值，而这种形式可能是纸币、硬币或电子支付。

通常情况下，由政府或其他权威机构发行和控制货币，但货币远不只是一种物理或数字的交换媒介。货币就像一种通用语言，使我们能够与世界各地的人进行交易，即使我们的语言和文化都不相同。



第二章

My
First
Bitcoin

HCM®

货币就像一种社会契约，它允许我们进行交换，而无需依赖以物易物或找到确实需要我们所提供物品的人。如果一群人开始接受巧克力作为大多数商品和服务的支付方式，那么巧克力就会成为货币(虽然在某些炎热的地方，巧克力作为货币可能相当糟糕)。

正如法国经济学家让-巴蒂斯特-萨伊指出：“货币在交换中只起一时的作用。当交易结束时，人们总会发现，是一种商品被换成了另一种商品。”

换句话说，货币本身并不能满足人类的需求，它只是让我们用一种商品交换另一种商品的工具。



交易是商品和服务的交换或转移，是两方或多边之间交换价值的一种方式。

交易存在许多不同的类型，从简单的交换(例如在熟食店买一个三明治)到更复杂的金融交易(如购买房屋或投资股票债券)，诸如此类。交易既可以当面进行，也可以通过电话、网络或其他方式进行，涉及个人、企业和金融机构等方方面面。

没有货币，这种交易会有多容易或可行呢？

你会用一头牛换取一百万颗草莓吗？

或者用60万颗草莓交换？那么5万颗呢？



来看这个短视频吧！



货币**是**交换商品的价值**依据**。

货币**不是**商品被交换的价值**本身**。

总之，货币：

可以促进贸易，因为每个人都接受货币作为最终支付手段。它使我们能够衡量不同商品和服务的价值并进行比较。接下来，让我们一起来看看货币的功能。

货币是什么？

2.2 货币的功能

货币在买卖商品和服务时扮演着关键角色。货币在世界上有如下几项重要功能。

1 价值存储

应长期保持货币的价值，使其成为人类劳动价值的一种储蓄和投资方式。这就让人们可以用货币来规划未来、借贷资金。因此，下一次，当你为一些特别的事情存钱时，请记住货币不仅仅是一种支付方式，还是一种可以帮助你计划和投资未来的工具。

你的价值 储存方式 是什么？		 比特币 (美元)	 黄金 (美元)	 美元 (欧元)
	2019年3月14日	\$3,846	\$1,293	€0.8817
	2020年3月14日	\$5,258	\$1,529	€0.90056
	收益/亏损	+36.71%	+18.25%	+2.14%

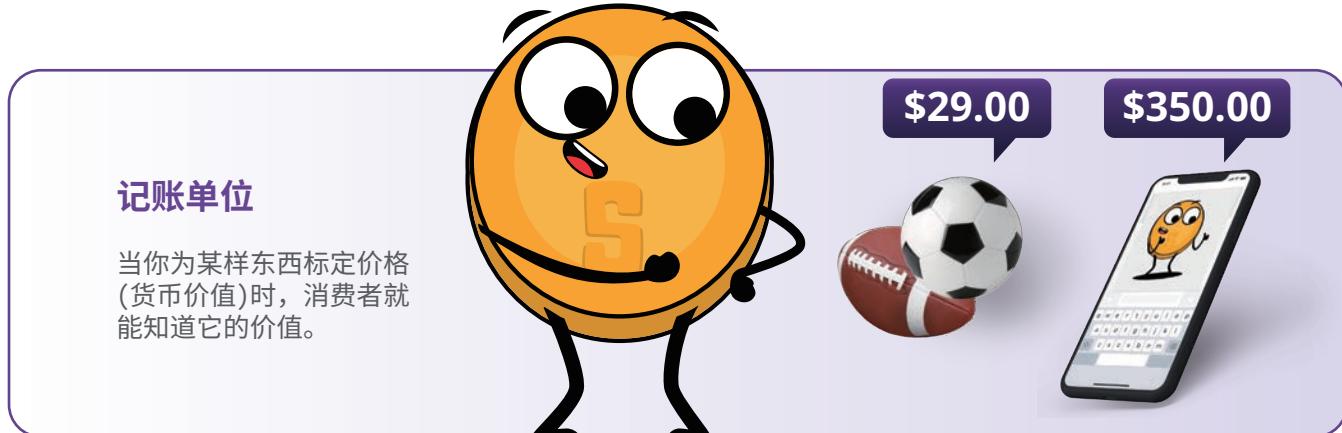
2 交换媒介

有了货币之后，你就不必非得去找一个正好想要你的东西的人以物易物。相反，你可以用货币买卖任何你想要的东西，这使得交易和商业变得更加方便和高效。



3 记账单位

货币提供了一个通用的价值标准，使人们能够表达和比较不同商品和服务的价格。这使得市场更加高效和透明，人们可以在知情的情况下做出买卖的决定。





第二章

试想一下：如果你想买一辆新车，那么你就可以比较不同经销商处车辆的价格，并根据以美元计算的价格来决定买哪一辆。可如果没有记账单位，你就不得不尝试用其他东西来比较一辆车和另一辆车的价值。比如，这辆车值多少头牛，或者制造这辆车需要多长时间。

正是这三种功能让经济变得复杂而充满活力。如果没有货币，商品和服务的买卖就会变得更加困难，我们的经济也难以发展。

课堂练习：这体现了货币的什么功能？

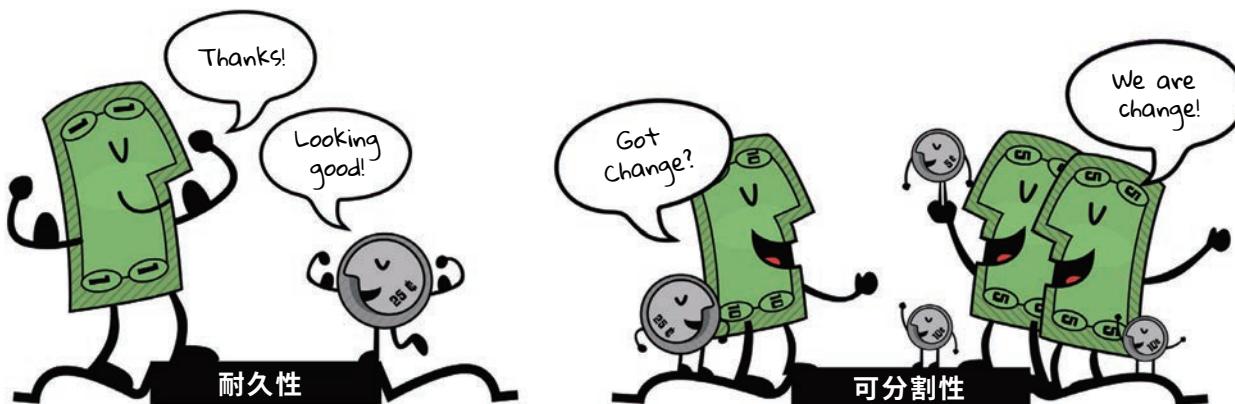
- ◆ 埃文决定把每周工资的一部分存起来，攒钱买一只小狗。
- ◆ 亚当在雷氏比萨店花8.30美元买了两片比萨。
- ◆ 马克无法决定是买75美元的音乐会门票，还是买95美元的滑雪通行证。

2.3 货币的特性

随着时间的推移，人们最终认识到，货币必须具备某些特质，才能作为有效的交换媒介。这些特性包括耐久性、便携性、可分割性、可替换性、稀缺性和可接受性。

◆ **耐久性**指货币抵御物理劣化和经久耐用的能力。这可以确保货币在可接受和可识别的状态下在经济中流通。黄金是一种经久耐用的材料，可以承受磨损，因此很好地体现了货币的耐用性特征。

◆ **可分割性**指货币被分割成更小单位的能力，这样人们就可以用货币来购买不同金额的物品。纸币可以很容易地被分割成较小的面额，因此很好地体现了货币的可分割性。



货币是什么？

● **便携性**指货币便于运输和携带。这使得人们可以毫不费力地使用货币买卖商品和服务。信用卡便于携带，可以很方便地放在钱包或皮包里，因此很好地体现了货币的便携性。



● **可接受性**指货币作为一种支付形式被广泛接受，人们可以放心地用货币来买卖商品和服务。美元作为一种支付形式被广泛接受，因此很好地代表了货币的可接受性特征。



● **稀缺性**指货币供应有限，这有助于保持货币的价值，防止我们花更多的钱来购买相同数量的商品。收藏邮票，尤其是稀有珍贵的邮票，可以使它成为一种很好的货币形式。因为这种邮票较为稀缺，而且可以随着时间的推移而升值。集邮者通常将邮票作为投资财富和分散投资组合的一种方式。



● **可替换性**指货币的可互换性，即一个货币单位等同于另一个相同价值的货币单位。货币应该是统一的。铜币的大小和重量都是统一的，因此很好地体现了货币的统一性特征。一美分总是一美分。



总之，这些特点使货币成了促进贸易和商业的有用而有效的工具，对经济的发展和稳定至关重要。



第二章

课堂练习

不同的资产具有不同的属性，并且在不同程度上发挥着货币的功能。最终，社会会根据稳定性、稀缺性、可分割性、可转让性和作为交换媒介的认可度等因素来决定将哪种资产用作货币。

要确定不同物品在多大程度上符合货币的具体特征，可以对每个物品的每个特征进行**1到5分**的评分。通过统计每个项目的得分，可以确定哪个项目最适合作为一种货币形式。

[0 = 糟透了; 3 = 还行; 5 = 好极了]

* 请不要填写“比特币”的这一栏；我们将在后续课程中回到这一部分。

使用下面的问题帮助你确定表格中的不同物品在多大程度上符合货币的特征。

-  **耐久性:** 该货币是否经得起长期磨损?
-  **便携性:** 该货币是否便于运输并能在不同地点使用?
-  **可替换性:** 该货币是否可以与其他形式的货币互换?
-  **可接受性:** 该货币作为一种支付形式，是否被广泛接受?
-  **稀缺性:** 该货币是否稀缺且不是太充裕?
-  **可分割性:** 该货币是否可以被分割成较小的单位进行交易?

良好货币的特性	 家畜	 香烟	 钻石	 欧元	 比特币
耐久性					
便携性					
可替换性					
可接受性					
稀缺性					
可分割性					
总分					

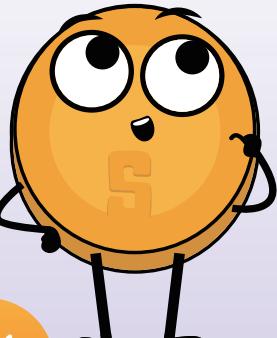
货币是什么？

2.4 货币的类型

货币可分为两大类：实物货币和电子货币。

实物货币包括：

- ◆ 法定货币，即由政府发行并被接受为交换媒介的纸币和硬币。
- ◆ 代用货币，代表对实物商品的债权。
- ◆ 商品货币，指具有内在价值并被广泛接受为交换媒介的实物，例如黄金和白银。



并非所有货币
都是一样的！

商品货币

代表性货币

法币



像火药这样的物品，就曾经被用作商品货币。



像这张银券这样的代表性货币，可以兑换成白银。



美联储票据如今是法定货币，联邦政府将其规定为一种可接受的债务支付方式。



数字货币：可以用于在线交易，包括电子货币、稳定币和加密货币。

电子货币：是普通货币(如美元或欧元)的数字版本，可以通过数字**支付通道**在线购买和出售商品。



支付通道是支持电子货币和其他数字资产从一个地方转移到另一个地方的基础设施。然而在传统金融体系中，总会有一个中介会收取费用并拥有接受、取消、撤销或延迟交易的权力，比如银行或金融机构。

在中介化的金融系统中，数字支付轨道的主要类型包括卡网络和数字钱包。前者在客户使用借记卡或信用卡购物时促进金融机构和商家之间的资金转移，后者则是允许用户存储和管理其电子货币，用户可以通过从其账户向接收者的账户转账来完成支付。



第二章

 My
First
Bitcoin

 HCM



中央银行数字货币 (CBDCs)

即一个国家法定货币的数字版本，由中央银行发行和支持，并由政府进行中介。



稳定币

一种数字货币，旨在保持相对某种资产(如美元)的稳定价值。



加密货币

是一种数字货币。有些加密货币是去中心化的，受规则约束；有些则是中心化的，由一小部分人控制。

归根结底，没有中间商的货币运作效率更高，对社会也更为有利，因为它可以防止少数人控制货币供应并集中权力。然而，创造这样一种无需依赖各方信任就能促进安全交易的货币，在历史上一直是一个挑战。要实现这一目标，就必须创造一种像互联网一样运行的货币。在这种货币中，控制权分散在每个人身上，同时又不分散在任何人身上。这就要求所有各方，包括掌权者，都同意为了更大的利益而放弃控制权。

2.5 货币心理学：稀缺性、时间偏好与权衡

想象一下，你被困在沙漠中，只剩下一瓶水。你很口渴，迫切地想喝水，但你也知道，在找到更多水之前，你需要这些水来维持生命。这就是一个典型的稀缺的例子——你只拥有有限的资源(水)，所以你必须选择如何使用它。在这种情况下，你可能会决定定量喝水，并在较长的时间内都只是小口喝水，以便让水能维持尽可能长的时间。

货币是什么？

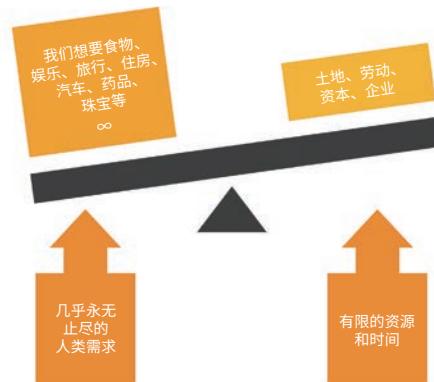


稀缺性迫使我们权衡使用资源的利弊，从而做出取舍。

或者，你也可以决定一次性喝下尽可能多的水，寄希望于水合作用的爆发给你带来寻找更多水所需的能量。在这种情况下，你需要在解渴和节约用水之间做出选择。而无论你做出哪种选择，都将面临一个艰难的决定。这种稀缺性的概念适用于各种资源，而并不仅仅是水。无论是金钱、时间，甚至是爱和关注，我们总是面临着关于该如何分配有限的资源的选择。

稀缺性有两种类型：人为稀缺性和自然稀缺性。

- 人为稀缺性：也被称为集中式稀缺性，包括限量版名牌包、稀有的球星卡和编号艺术品等。这些物品很容易被复制或伪造。
- 自然稀缺性：也被称为非集中式稀缺性，其中包括盐、贝壳和黄金等贵金属。这些东西较难被复制或伪造，二者之间最大的区别在于控制。



集中式稀缺由公司或政府等单一实体控制，而分散式稀缺不受任何人控制。对清洁水等基本资源的控制就是集中式稀缺的一个例子，这种稀缺对穷人影响尤为严重。在一些地区，清洁水的获取由私营公司或政府实体管理，它们可能会限制清洁水的分配，从而导致这一重要资源变得稀缺。这种集中控制可能会导致价格上涨或获取清洁水的机会不平等，贫困社区往往首当其冲。获取清洁水的机会有限不仅会影响他们的健康和福祉，还会使贫困永久化，因为他们可能被迫支付更高的水价或通过长途跋涉来获取水源。

稀缺性影响着我们的选择。了解稀缺性可以改善我们的决策。我们经常需要在眼前利益和长远利益之间做出选择，正是这些权衡决定了我们实现目标的路径。



时间偏好指人们往往会选择现在就拥有某些东西，而不是以后。





第二章



一个时间偏好的例子：

比如，你可以选择在今天得到100美元，或者一年内得到110美元。如果你的时间偏好很高，你可能会选择今天就得到 100 美元，因为你更看重的是现在拥有这笔钱所带来的直接满足感，而不是等待一年后多得到 10 美元的潜在好处。另一方面，如果你的时间偏好较低，那么你可能愿意等待未来的更大回报，因为你不太在乎眼前的满足感，而是更加注重长期规划。

活动：时间偏好

高时间偏好 VS 低时间偏好

- 1 听老师讲解该如何选择糖果。
- 2 决定是现在就领取一颗小糖果或棉花糖，还是等到下课时再领取两颗糖果或一颗更大、更好的糖果。
- 3 做出决定，并让老师知道你的选择。根据自己的决定，在现在或下课后去领取糖果。
- 4 参与关于该活动的全班讨论，反思自己的决策过程和时间偏好概念。

结论和讨论

- 是什么因素影响了你决定是现在就吃糖，还是等待之后获得更大的奖励？
- 活动结束后，你对自己的决定有何感想？
- 在现实生活中，高时间偏好可能有害，低时间偏好可能有益。思考一下，你能举出这样的例子吗？
- 选择高时间偏好而不是低时间偏好可能会产生什么潜在后果？

在沙漠的例子中，高时间偏好就意味着你可能更倾向于立即喝光所有的水，即使这代表你之后就没有水喝了。你之所以这样选择，是因为对你来说，现在感到的口渴比你将来可能感到的口渴更为迫切。

另一方面，如果你选择定量地喝水，并且在一段时间内把水慢慢喝完，那么你表现的就是一种比较低的时间偏好。这意味着为了获得更大的长期生存的机会，你愿意等待一段时间再来解渴。

货币是什么？



机会成本指你在做决定时放弃的一个接下来的最佳的选择的价值。
每一个决定都有利有弊。

今天的选择



购买7美元一杯的草莓奶昔

现在



将这7美元用于其他用途

未来



通过定期储蓄这7美元受益

在沙漠的例子中，立即喝掉所有水的机会成本，是你通过定量饮用和长期使用这些水而获得的生存利益。

比方说，你决定定量喝水，并在较长的时间内小口喝水。这样一来，你就能拥有足够的能量和水分去寻找更多的水。然而在寻找水的过程中，你遇到了一株仙人掌，里面有少量的水。虽然并不是很多，但也足够你暂时解渴了。而如果你之前的决定是一次性喝完所有水，那么你可能就没有足够的能量去寻找更多的水，以及发现仙人掌了。

在这个例子中，一次性喝完所有水的机会成本就是找到仙人掌并且补充更多水分的机会。

这个例子说明，机会成本不仅涉及两个选择之间的直接权衡，也包含我们的选择可能带来或失去的潜在的未来机会。

我们是否愿意放弃为了眼下更小的回报，放弃未来更大的回报？这受到我们时间偏好的影响。或者说，即时满足和长远的规划，我们认为哪一个更有价值。

在本章，我们探讨了货币的基本概念。本章的内容涵盖货币的定义、功能、性质和各种类型。我们讨论的一个重要方面，是了解货币心理学，重点是稀缺性、时间偏好和权衡等概念。这一探索为理解金钱的复杂本质及其在我们生活中的作用奠定了基础。在下一章中，我们将讨论货币的历史以及货币是如何随着时间的推移而演变的。

第三章

货币的历史

3.0 引言

活动: 以物易物游戏

3.1 从以物易物到现代货币的演变

3.1.1 早期货币形式存在的问题

3.1.2 硬币和纸币的发展

3.1.3 从“稳健货币”到“不稳健货币”的转变

3.1.4 从纸币到银行卡

3.2 数字货币

货币的历史

3.0 引言

货币不是被设计出来的，而是在市场过程中产生的。
货币不是由政府创造的，而是随着时间的推移，作为一种自发秩序出现。

默里·罗斯巴德



想象一下，在很久以前，人们还没有现在所使用的硬币或纸币。那时，他们有一种独特的交易方式——用贝壳或黄金等贵金属作为一种特殊的货币。这听起来可能很奇怪，但这就是他们的货币——一种大家都认为有价值的东西。在本章中，我们将踏上时间之旅，亲身经历货币的演变。我们将追溯货币的起源，观察货币在历史长河中的变化和调整。

活动: 课堂练习 - 以物易物游戏

老师给了你们一张小纸片。你的目标是在历史商业游戏中用你“拥有”的东西来交换你“想要”的东西。请在纸片的上方清楚的写上你的名字。

第一轮: 以物易物

现在是公元前 6000 年，毫无疑问，我们所知的货币还没有发明出来。现在，你们身处美索不达米亚，正通过以物易物的方式直接对商品和服务进行交换。

顺便提一下，现在许多企业仍然接受非货币支付的服务。政府在报税时，会将这些以物易物的交易与货币交易同等对待。

沿虚线剪下纸张。你的目标是尽可能多次地交换你所“拥有”的东西，最终得到你最初“想要”的东西。但你不能改变自己最初“想要”的东西。接下来，你有 5 分钟的时间可以用来完成这个练习的目标。



第三章



当你新“拥有”的东西与你最初“想要”的东西相符时，请回到座位上。时间截止后，如果你还没有找到交易伙伴，也请返回座位。



如果你在一次交易后就得到了自己想要的东西，请举手。或者你是在两次或三次交易后才得到的？

简短但具体地回答下列问题。

1. 为什么你们中有些人能够找到交易对象，其他人却不能？

2. 以物易物有什么好处？

3. 根据你的经验，使用易货贸易有哪些缺点？



第二轮：商品货币

快进到公元前14世纪左右的非洲西海岸。此时，以物易物变得繁琐而低效。我们的文明不断发展，现在已经进入了使用商品货币的阶段。

货币的历史

为了简单起见，老师给了你们一份通心粉。我们假设按照惯例，每种物品的价格都是一份通心粉，你的目标是获得你“想要”的东西。但现在，我们人类变得更加聪明，并找到了解决这种问题的方法。

- 为什么我们将通心粉视为商品货币？
 - 我们现在该如何得到想要的东西？
 - 通心粉容易加工吗？
 - 为什么说货币取代了商品？
 - 货币在哪些方面比以物易物更有效率？
 - 使用通心粉作为货币有什么缺点？
 - 你认为当西班牙开始把一船一船的通心粉运往美国社区(将金银从美洲运回西班牙)时，发生了什么？
-
-
-
-
-
-
-

3.1 从以物易物到现代货币的演变

3.1.1 早期货币形式存在的问题



观看这个短视频，了解《纸币的历史》系列中的“交换的起源”。

在易货经济中，人们根据各自提供的商品和服务的相对价值进行交易。但易货经济效率低下，且难以管理，在复杂的社会当中更是如此。

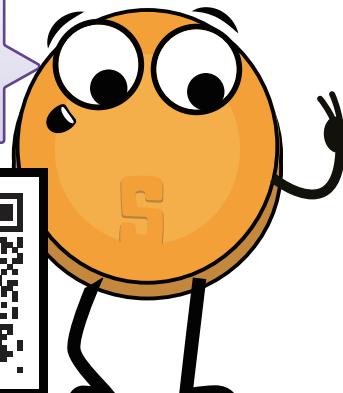
在任何以物易物的制度中，都必须存在一种被称为“**需求的双重巧合**”的情况——因为人们必须总能找到既有自己想要的东西，又想要自己所提供的东西的人。



让我们假设

- 约瑟夫想用他的香蕉换雅尔的椰子。
- 但雅尔只想用她的椰子换塔米的芒果。
- 而塔米只想用自己的芒果换约瑟夫的香蕉。由于没有需求的双重巧合，他们陷入了一场永无休止的水果交易循环中。
- 约瑟夫建议他们用水果换一杯冰镇苏打水，但他们马上意识到自己身处偏远小岛，根本没有苏打水。
- 于是，他们决定就坐在沙滩上，静静地享受他们的水果。
- 使用共同的记账单位，如“苏打”等，可以大大提高贸易和商业的效率。在古代，人们开始使用珠子、贝壳，以及其他在社会中具有价值的物品作为交换媒介。

第二集名为
《不仅是面条》，
来自《纸币的历史》。



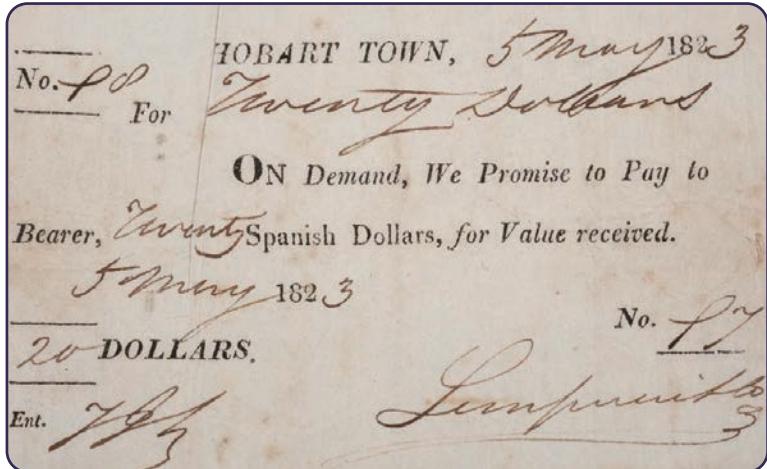
3.1.2 硬币和纸币的发展

随着你和你的社区越来越多地参与贸易和商业活动，你逐渐意识到了以物易物和其他非货币交换形式的局限性。于是，你决定使用金属硬币作为货币形式。



商品货币是用金银等贵金属材料制成的货币。在历史上，这些货币曾被用作价值储藏手段、交换媒介。在遥远的过去，它们甚至还曾被用作记账单位。

货币的历史



然而，当你开始更加频繁地使用金属硬币时，你遇到了一些弊端——它们可能很重，在大宗交易中携带不便。而且你注意到有些人在利用这个系统的漏洞：他们将硬币熔化，再与更便宜的金属混合，制造新硬币，从而导致价格上涨，破坏了人们对这个系统的信任。

为了解决这些问题，你和你的社区开始以纸质票据作为货币形式。这些纸质票据源于古代中国，是一种方便且易于兑换的货币形式。它们由黄金和其他贵重金属支持。在十七世纪到十九世纪期间，这些纸质票据可以被兑换成这些金属。这样一来，您就可以拥有一种更便携、更易于转移的货币形式，同时还能保持贵金属的价值和安全性。

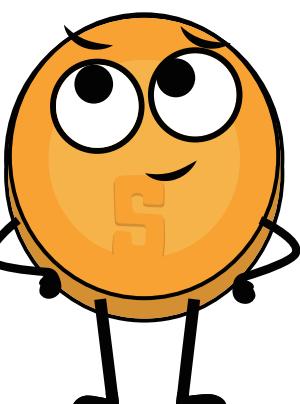


3.1.3 从“稳健货币”到“不稳健货币”的转变

时间快进到17世纪的瑞典。现在，你已经完全依赖银行来存储自己的宝贵资产。然而，你开始注意到这些银行家的猫腻——他们发行的纸质票据似乎比他们储存的黄金更多，这使得他们创造的货币比这些的票据背后的资产还要多。这种偷偷摸摸的做法，可以让银行家们从纸质票据的价值和他们为客户持有的黄金价值之间的差额中获利。



当你真正尝试将纸币理论付诸实践时，会发生什么呢？
在《纸币的历史》第四集中
了解答案吧。





第三章

你意识到，这标志着货币运作方式的重大转变——正在从一个稳健的货币体系（即由贵金属支持的货币），转变为一个不稳健的货币体系（即法定货币没有实物商品支持）。这一转变并非一蹴而就的，而是一个受多种因素影响的渐进的过程。工业革命带来了大规模的生产和城市化。不仅如此，银行和股票市场等先进金融体系的发展也起到了一定作用。中央银行和其他货币管理机构的出现促进了货币的集中化或控制，导致以法定货币的发行来支持经济的增长。

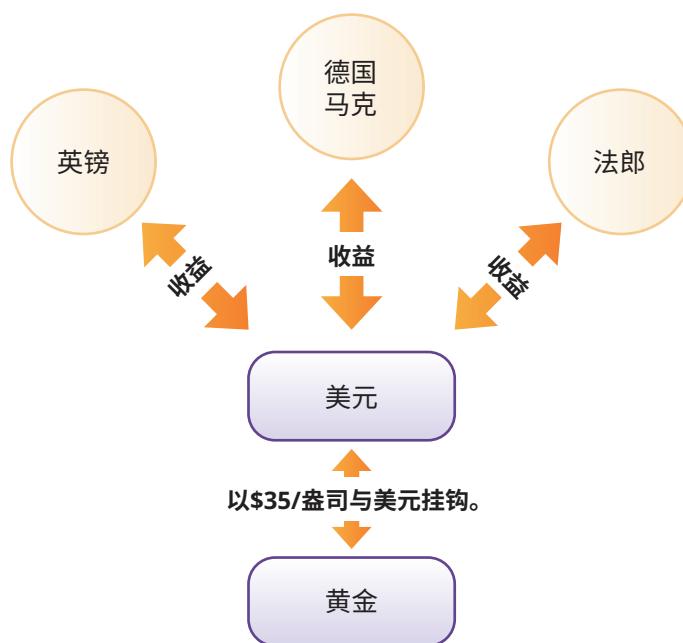


然而，你逐渐看到了这种**中央集权的弊端**——包括不负责任的消费、**债务增加**，以及通过经济激励来操纵公民。

在第一次世界大战之前，你可以将纸币兑换成预设数量的黄金。但两次世界大战和1929年的经济危机结束了这一局面。1944年，布雷顿森林协议签署，确立了美元作为世界储备货币的地位，并将美元的价值与黄金价格挂钩，将黄金固定在每盎司35美元的水平上。而其他国家的货币与美元挂钩，这有助于稳定国际金融市场。

布雷顿森林体系

(1945—1972)



不幸的是，这一体系在20世纪60年代末开始瓦解，并导致了1971年的尼克松冲击。当时美国政府中止了美元对黄金的可兑换性，这标志着金本位制的终结。同时，一个以创造和积累债务为驱动力的世界开始了。

在日常生活中，你开始注意到，货币的价值已不再像以前那样稳定。就像一把有弹性的尺子难以准确地测量桌子的长度一样，生活在一个货币价值受制于当权者的、不可预测性的世界里，你也会难以准确衡量商品和服务的价值。身处一个货币价值不再与黄金等实物商品挂钩的世界里，你会感到困惑甚至不安。

货币的历史

你看到了这一转变对全球经济的影响，并开始质疑法定货币的稳定性和可靠性。此刻你意识到，在现代世界中，美元的价值不再像与黄金挂钩时那样固定不变，而是会出现波动。美元的价值会受到各种因素的影响，包括通货膨胀(不断上涨的物价)、利率、国家经济实力、政治事件、市场投机和国际贸易需求等，这导致美元作为记账单位变得更加困难。这可能是一个令人困惑且难以预测的时期，因为你需要努力驾驭不断变化的美元价值及其对你日常生活的影响。

尽管人们努力通过现代货币制度、提高效率、增加获取信息的机会和加强沟通来提高生活质量，但大多数人的生活水平还是开始由于以下原因下降。

- 滥用中央集权
- 物价上涨
- 实际工资停滞不前
- 货币疲软
- 需要花更多的钱来买更少的东西

对于那些经济资源较少的人来说，这无疑是个挑战。他们获得教育、信贷、资源、社会网络和政治代表的机会可能有限，这导致他们可能在成功的能力方面处于不利地位。

结果就是，富人似乎不断变得更富，穷人则不断变得更穷。



3.1.4 从纸币到银行卡

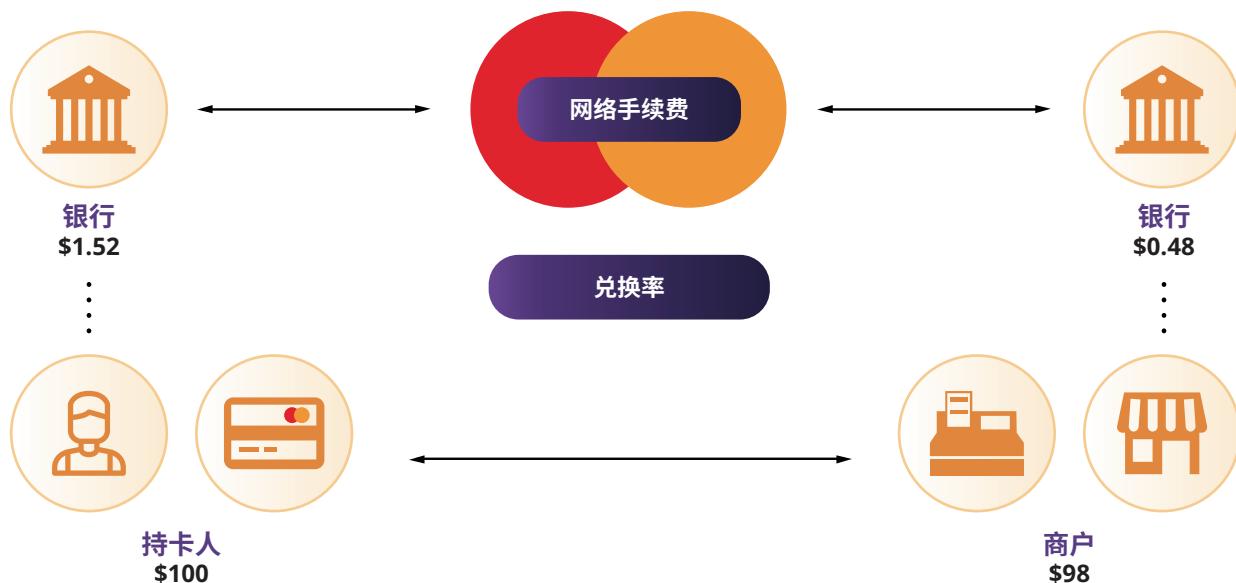
从第一张信用卡在 20 世纪 50 年代问世至今，我们已经走过了漫长的道路。只需轻轻一刷，我们就能随时随地买到任何想要的东西，没有任何麻烦。这就像为我们打开了一个充满无限可能的世界，让人兴奋不已。殊不知，我们对信贷的依赖会带来痛苦的后遗症——比如提高商品的总体成本，来刺激某种注定要失败的经济。



第三章

My
First
Bitcoin

HCM



随着技术的进步，我们处理金钱的方式也在发生变化。网上银行和电子商务网站的出现使得完全在线管理和消费成为可能。

数字货币的兴起标志着这一演变过程中的又一次重大飞跃。数字货币为我们提供了新的可能性，并重塑了我们的金融交易方式。

3.2 数字货币

现在，让我们进入令人兴奋的数字货币世界。与传统货币不同，数字货币仅以电子形式存在。数字货币使用计算机和特殊软件进行存储和交换。

数字货币允许个人通过互联网发送资金。就像电子邮件可以让我们即时发送信息且无需运费一样，数字货币可以让我们即时发送和接收价值，且成本极低。

我们今天使用的货币正变得越来越数字化。实际上，只有一小部分货币以硬币和纸币的形式存在。银行和银行服务为用户提供通过互联网无缝交换货币的应用程序。但是，钱是从哪里来的呢？

在本章中，我们见证了从以黄金为代表的稳健货币到以纸币为代表的不稳健货币的转变，以及现在的数字法定货币。在下一章中，我们将探讨当前的法定货币体系是如何形成以及如何运作的。

第四章

什么是法定货币? 法定货币由谁控制?

4.0 引言

4.1 法定货币简史

4.2 法定货币系统

 4.2.1 法定货币体系

 4.2.2 部分准备金银行制：由债务推动的系统

活动: 部分准备金银行制

 4.2.3 谁控制着法定货币系统？他们该如何从中获益？

4.3 中央银行数字货币：法定货币的未来

什么是法定货币？ 法定货币由谁控制？

4.0 引言

人类的历史就是货币贬值的历史。

米尔顿·弗里德曼

在上一章中，我们看到了货币是如何随着时间的推移而演变的，以及我们的货币体系是如何从稳健货币过渡到不稳健货币，进而塑造了我们今天生活的世界的。本章将深入探讨这些发展是如何塑造今天的法定货币体系，以及法定货币体系是如何运作的。

那么，这个法定系统是什么样的？它又是如何产生的呢？

要回答这个问题，我们首先需要关注美元。美元是当今世界的储备货币，在当今世界发挥着主导作用。每个国家都会直接或间接地感受到美元决策的影响。要真正了解法定货币体系在贵国的运作方式，就必须解开贵国与法定货币体系的发源地——也就是美国，之间的历史渊源。

4.1 法定货币简史

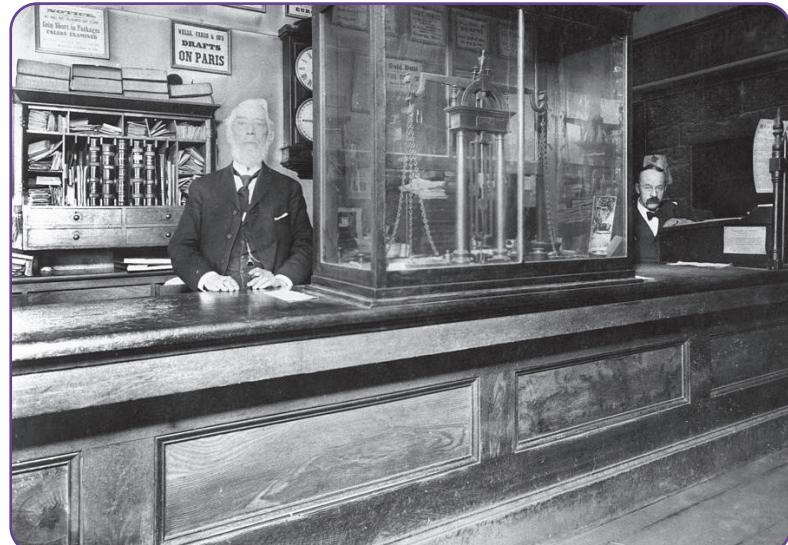
1815—1933	1913	1933	1934	1944	1971	1980
金本位制度	成立名为“美联储”的中央银行	第6102号行政命令。每个公民都必须按照每盎司20.67美元的汇率上缴黄金	《黄金储备法》通过将美元贬值40%至每盎司黄金35美元，从人民手中窃取财富	布雷顿森林协定：美元成为世界主要储备货币	尼克松冲击，美元对黄金的可赎回性的终止，催生了法定货币体系	黄金的价值从1970年的35美元/盎司，上升到1980年的870美元/盎司，这使得人们的钱在短短10年间贬值了96%

时间轴

19世纪，全世界的文明都以健全的货币本位为基础，并使用金银等贵金属，因为这些贵金属稀缺、耐用、易识别。随着全球贸易的增长，携带大量金属变得具有挑战性，于是就出现了金银仓库。这些仓库安全地储存着人们的贵重金属，并为人们提供可兑换特定数量黄金或白银的纸质证书。作为存放资金的交换，个人收到的纸质证书与他们存放的黄金或白银数量直接挂钩。纸质证书与有形商品货币之间的这种直接联系标志着我们现在所认识的银行的早期阶段。



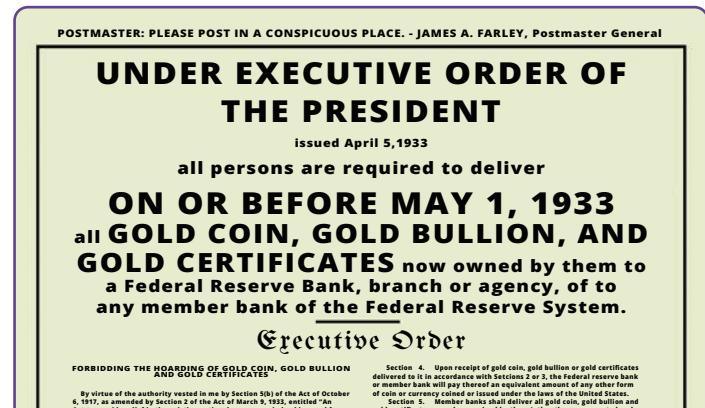
第四章



起初，银行的目的是保护客户的资金，后来却用其从事高风险的借贷行为，为他们没有的黄金签发证书。如果有太多客户同时领取他们的钱，那么这种做法就会造成银行挤兑的威胁。为了应对这一风险，银行与政府合作，建立了一个使再贷款合法化的体系。1913年，他们成立了美联储，这是一家中央银行，负责发行新纸币以及救助陷入困境的银行。在全球范围内，各国政府都认识到了黄金和白银的价值，从而引发了争夺黄金和白银控制权的冲突和战争。在第二次世界大战之前的岁月里，列宁、斯大林、丘吉尔、罗斯福、墨索里尼和希特勒等领导人均出于战略目的选择了攫取黄金。

20世纪30年代初，美国以资产支持货币的方式发生了重大变化。当时，人们曾经以黄金的形式持有大量财富。然而在1933年，罗斯福总统发布了第6102号行政命令，要求每个公民放弃黄金。这并不是一次自愿的交换——人们被要求交出自己的黄金，如果拒绝，他们将面临严厉的惩罚。

政府将汇率定为每盎司黄金20.67美元。这意味着，人们每拥有一盎司黄金，就能获得相当于20.67美元的纸币。人们不得不接受这些纸币，希望有一天能够将它们换回自己的黄金。

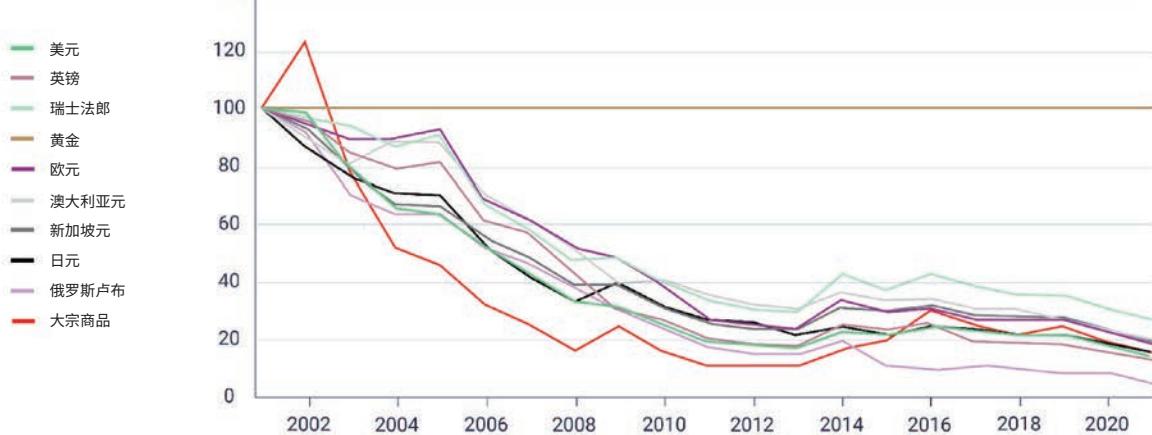


什么是法定货币？ 法定货币由谁控制？

1934年，《黄金储备法》允许人们再次用纸币兑换黄金——然而，这一切是有陷阱的。政府故意让纸币贬值，并将汇率提高到每盎司黄金35美元。这一贬值打击了中下层辛勤工作的人们，因为这意味着由于纸币贬值，他们曾经的积蓄也大大贬值。

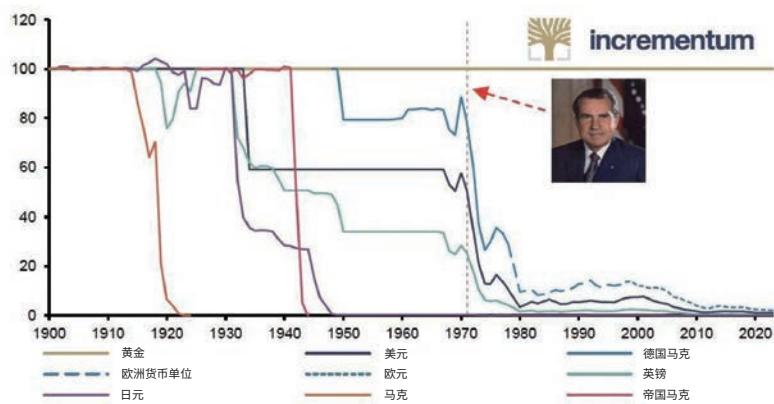
第二次世界大战结束，签订于1944年的布雷顿森林协议确立了美元作为世界储备货币的地位，并且美元可以直接兑换黄金。然而，1971年尼克松总统终止了美元与黄金的兑换关系，从而切断了美元与黄金之间的联系。这标志着一个重大的转变，即货币的价值不再由黄金等实物商品来支持，而是由使用货币的人们的信任和信心来支持。由于各国政府和中央银行保留了人民的大部分黄金，黄金价值飙升，并于1980年达到每盎司870美元。

以金衡盎司
计算的价值



总之，人类社会从稳健的货币标准过渡到不稳健的(法币)标准这一过程，这就是政府和银行从公民手中攫取贵金属的故事。真正的钱最终落入了政府和银行的腰包，而人民只能得到一张纸，其唯一的价值来自政府的强制使用。

以黄金衡量的黄金及各类货币 1900-2023



来源：世界黄金协会(World Gold Council)、路透社(Reuters Elkon)、incrementum AG



第四章



4.2 法定货币系统

传统货币的根本问题在于让它发挥作用所需的信任。人们必须相信中央银行不会使货币贬低，但在法定货币的历史上，这种信任被破坏的例子比比皆是。

中本聪

从由多数人控制的健全货币，过渡到由少数人控制的不健全货币，这个系统究竟是如何运作的呢？

4.2.1 法定货币体系

法定货币体系的特点是通过法定货币法律强加给人们的强制性。“Fiat”一词源自拉丁语，意思为“法令”，代表当局发布的指令。

与黄金等有形资产支持的货币不同，法定货币缺乏这种支持。相反，对法定货币的使用是由法律规定的。美元、欧元、英镑、人民币、比索等日常货币都属于法定货币。

法定货币法：规定所有公民必须接受某种货币的法律。



法币的价值在于人们相信它可以兑换商品和服务，并幻想它能长期保持其价值。法币好比一张音乐会门票，它的价值不在于纸质门票本身，而在于乐队(政府及其中央银行)会带来精彩表演(提供经济稳定)的保证。

法币的优点

- ✿ **使用方便：**法币便于日常交易。
- ✿ **降低成本和风险：**法币不像黄金那样需要重重保障，因此更加便宜、安全。

法币的弊端

- ✿ **通货膨胀风险：**物价可能持续上涨，以致通货膨胀，历史上曾出现过恶性通货膨胀。
- ✿ **集中控制和操纵：**小团体可以影响和操纵系统，导致审查和没收。
- ✿ **对手风险：**如果政府面临挑战，货币就会贬值。
- ✿ **滥用的可能性：**系统可能被滥用，导致腐败，以致失去信任。

什么是法定货币？ 法定货币由谁控制？

商品与货币：描述二者区别

请记住：在法定货币出现之前，政府会用贵重、稀缺、难以获得的实物商品(如黄金或白银)铸造硬币，或者印制纸币，用以兑换一定数量的实物商品。这就是商品支持系统。

现在，在法定货币体系中，货币更像大富翁的钱。法定货币体系中的货币由中央银行印制的纸片组成，政府的政策会直接影响其价值。政府和中央银行基本上就是“垄断游戏的银行家”，他们掌控着游戏的运作方式、谁能得到什么，以及价值多少。换句话说，政府承诺会做好对货币系统的管理工作。

总之，法定货币之所以有价值，只是因为政府强制使用它们；但法定货币本身没有任何效用。

总之，法定货币体系是一场信任游戏。在这场游戏中，我们货币的价值取决于掌权者的承诺，而人们只能寄希望于政府为所有人的利益而行动。接下来，我们将了解银行如何制造新货币、谁参与其中，以及对经济的影响。

4.2.2 部分准备金银行制：由债务驱动的系统

幸好全国人民不了解我们的银行和货币体系，因为我相信
如果他们了解的话，在明天早上之前就会产生一场革命。

亨利·福特

部分准备金制银行业务是法币体系的主要组成部分之一，它允许银行将客户存款的很大一部分贷出。你有没有想过，为什么银行要为客户提供这么多服务？银行虽然看起来似乎很慷慨，但重要的是我们要记住，银行也是企业，其首要目标是盈利。但如果他们是通过让人们借钱来发放资金，那他们又是如何盈利的呢？

除了赚取存款利息外，银行还通过其他方式创收，包括：

- 对发放的贷款收取利息。
- 收取自动取款机使用费和账户维护费等服务费。
- 通过投资赚钱，如买卖证券或投资房地产。
- 保留一定比例的贷款准备金，将其余部分用于投资或放贷。
- 支付存款利息，收取支票和储蓄账户费用。

银行收到一笔存款后，只需保留一部分(准备金要求)，
其余部分可以贷出。



银行以一定利率从存款人处借款

(例如5%)



银行以更高的利率
将这笔钱借给借款人
(例如9%)



银行通过贷款获得的利息支付存款利息

(9% - 5% = 4%)

其余部分作为利润留存



第四章



例如，如果你存入 100 美元，而准备金要求为 10%，那么银行就可以借出 90 美元，只保留 10 美元作为准备金。借款人将 90 美元存入另一家银行，循环往复。尽管最初只有 100 美元的存款，但在经济中，货币总量增长到了 271 美元，而且似乎是凭空出现的——这种现象被称为乘数效应。

这一过程促成了债务驱动的货币体系，因为银行总会通过每笔贷款创造新的货币，从而增加总体货币供应量。随着部分准备金银行业务的继续，经济中的债务总额会上升，进而导致通货膨胀。

该系统依赖通过借贷创造货币的持续循环，就像为吸毒者提供稳定的毒品一样。然而，如果银行贷出的钱超过其储备，而储户同时急于取款，那么银行就可能面临倒闭。

在这种情况下，中央银行作为最后贷款人进行干预，提供新货币以防止银行倒闭。中央银行通过回购资产或直接向银行账户注入货币来实现这一目的。实质上，通过中央银行不断注入新货币，银行才免于倒闭。这种由中央银行系统性拯救的、以债务为动力的系统导致了经济的繁荣与萧条的循环。

想象一下，你有一个朋友也是银行家，我们就叫他达克斯吧。

达克斯喜欢自行车，他想借你的自行车，因为他有很多地方要去。于是你把自行车借给了他，可没想到达克斯同时也同样向其他许多朋友承诺借自行车。有了你借给他的那辆真实的自行车，达克斯设法创造了更多想象中的自行车，并开始把它们借给朋友们。他的每个朋友都以为自己可以随时享受骑车的乐趣，但问题是，真正的自行车只有一辆！而其他的自行车都是想象出来的，只是承诺而已。

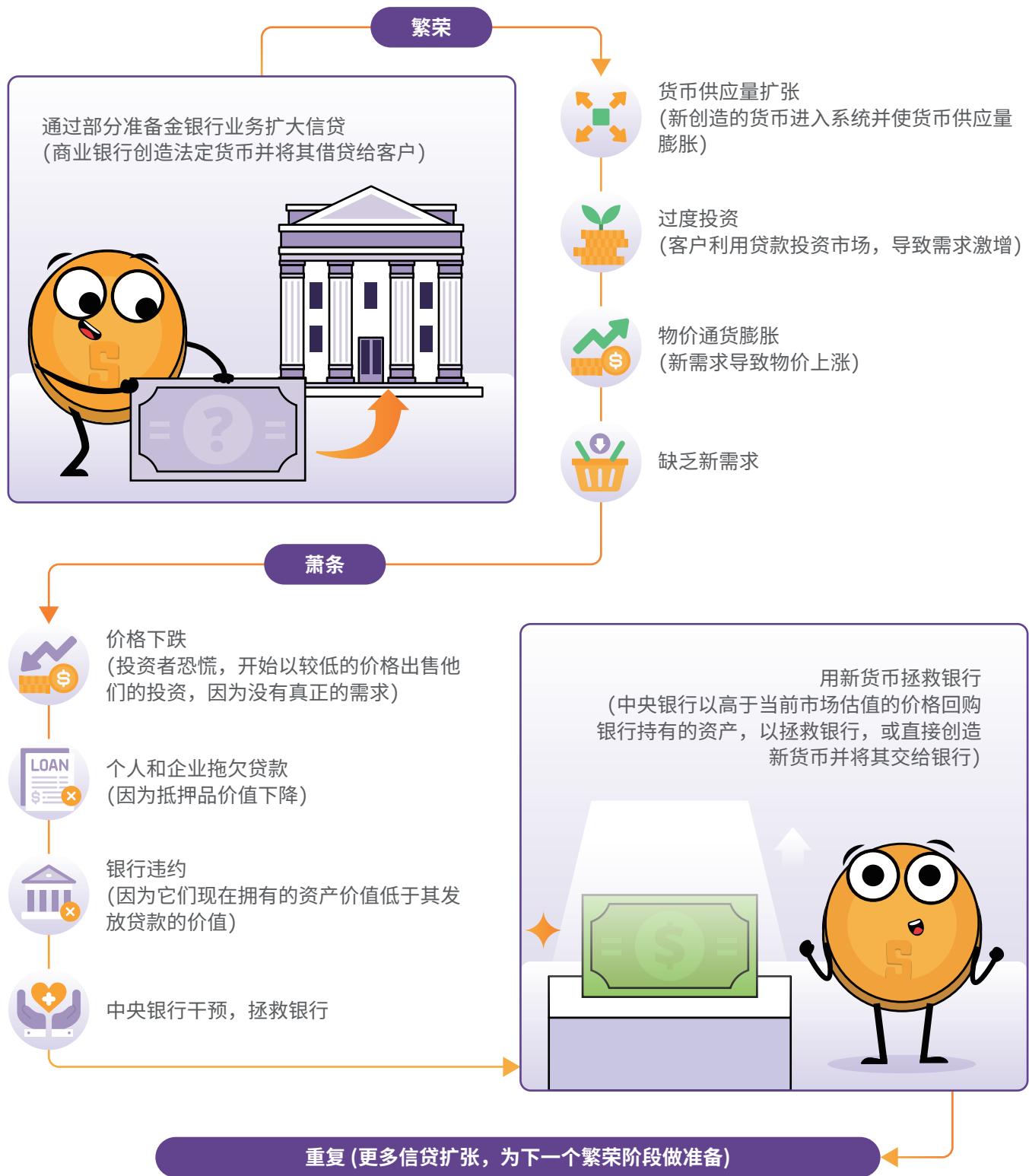
那么，会发生什么呢？随着更多想象中的自行车流通起来，每个人都非常高兴——至少在最初是这样。因为一开始，没有人会在同一时刻使用自行车。这看起来没有问题，感觉每个人都有大量的自行车。于是，所有朋友都开始制定更多的计划，畅想自己要骑着自行车去的所有地方。

然而，魔力就在这里开始失去魅力。在一个阳光明媚的日子里，大家都觉得今天是骑自行车的好日子，于是，他们都出现在达克斯家门口，兴奋地骑着想象中的自行车兜风。但是，现实摆在面前——真正的自行车只有一辆。失望接踵而至，承诺的骑行价值突然大打折扣。

在部分准备金贷款的世界里，情况也是如此。银行贷出的钱比其实际拥有的多，一时间，人人都享受了好处。更多的钱流通了起来，人们似乎有很多钱可以周转。但是，如果有太多人同时想把钱取出来，那么其真正的价值就会显现出来：没有足够的钱来兑现所有承诺。

这种情况会影响共同利益和个人的价值。丰收的承诺变成了一场骗局。当每个人都想拥有一辆真正的自行车时，想象中的自行车就会失去其感知价值。当这种情况发生时，人们会发现他们存在银行里的钱并不是真的，而这就会导致恐慌、银行挤兑，甚至整个经济的崩溃。截至目前，为这些崩溃买单的始终是同一个群体：世界上的中下层阶级。

什么是法定货币? 法定货币由谁控制?





第四章

活动： 部分准备金银行制

在下面的练习中，我们将探讨部分准备金银行业务是如何导致货币贬值、通货膨胀和购买力下降的。我们将使用一个简化的例子，这个例子涉及六个参与者，其中一个将充当银行，一个是我们今天仍在大量使用的准备金率：10%。

- ✿ A 刚从彩票中赢了 100,000 美元，并将其存入银行 (B)。在 10% 的准备金率下，B 必须在其金库中保留 10,000 美元，并能够将剩余的 90,000 美元贷出。
- ✿ C 从 B 处借了最高限额(90,000 美元)，并用这笔钱从 D 处买了一栋房子。
- ✿ D 将从 C 处收到的 90,000 美元存入银行 (B)。现在银行持有的存款总额为 190,000 美元。
- ✿ E 向 B 申请贷款，银行贷出了新存款的 90%，即 81,000 美元。
- ✿ E 用 81,000 美元的贷款从 F 处购买了一件艺术品，然后把钱存入银行(B)。现在银行所记录的存款总额为 271,000 美元。

在这种情况下，最初的 100,000 美元存款在经济中流通后共产生了 271,000 美元存款。

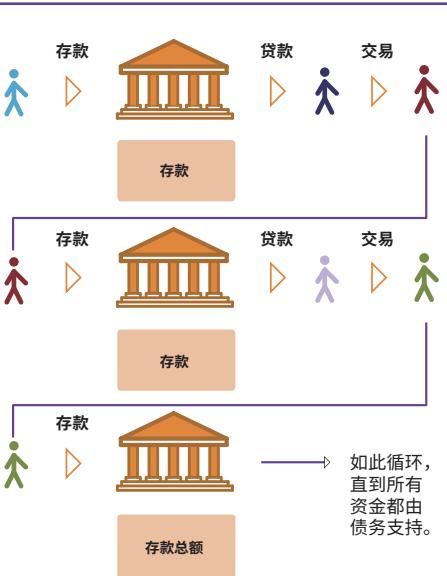
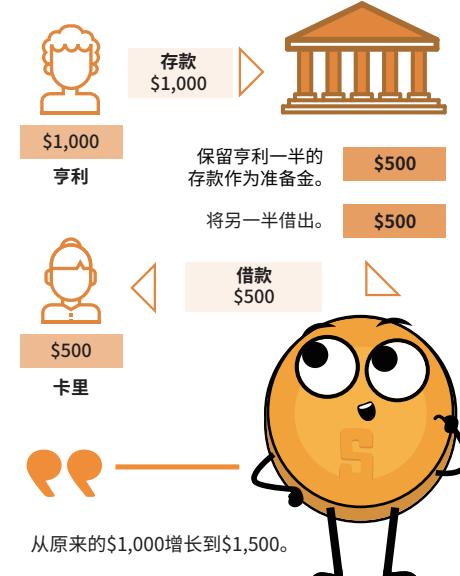
如果存款准备金率降低到1%，那么其创造的货币量将大大增加 ($100,000 \text{ 美元} / 0.01 = 10,000,000 \text{ 美元}$)。在这种情况下，如果货币继续在整个经济中流通，那么这 10 万美元实际创造了多少货币？

值得注意的是，为了刺激经济，美联储(美国中央银行)从2020年起将存款准备金率降至零。

我们需要以下志愿者：

- A = 存款人(彩票中奖者)(浅蓝色)
- B = 银行出纳员(银行)
- C = 债务人#1(深蓝色)
- D = 财产所有者/存款人(红色)
- E = 债务人#2(浅紫色)
- F = 艺术画廊所有者/存款人(绿色)

部分准备金银行制度 保留1/2



什么是法定货币？ 法定货币由谁控制？

4.2.3 谁控制着法定货币系统？他们该如何从中受益？

主要有四个参与者：政府、富人、金融部门和中央银行。它们共同控制着货币系统。

政府

政府就像“法币秀”的导演。除了收税，政府的资金还来自财政部发行的新债（债券）。当对这些债券的需求不足时，剩余的债务就由中央银行购买。这意味着他们可以继续从事他们的活动，追求他们的利益，而不需要人民的批准。这就像获得一张不用担心立即偿还的信用卡。这看似对政府有利，但对其他人来说是有代价的。

富人

富有的人从法定货币体系中获益良多。有了积累更多债务的能力，他们就可以投资商品、房地产和股票等资产，从而几乎毫不费力地创造新的财富。

金融部门（银行）

银行和其他金融机构并不直接控制法定货币体系，却从中受益匪浅。由于无需承担责任，他们可以通过部分准备金贷款来追求并加速创造新货币，并从更高的收入中获益。银行几乎不用承担任何后果，因为它们会得到新的法定货币的救助，以防止整个系统崩溃。

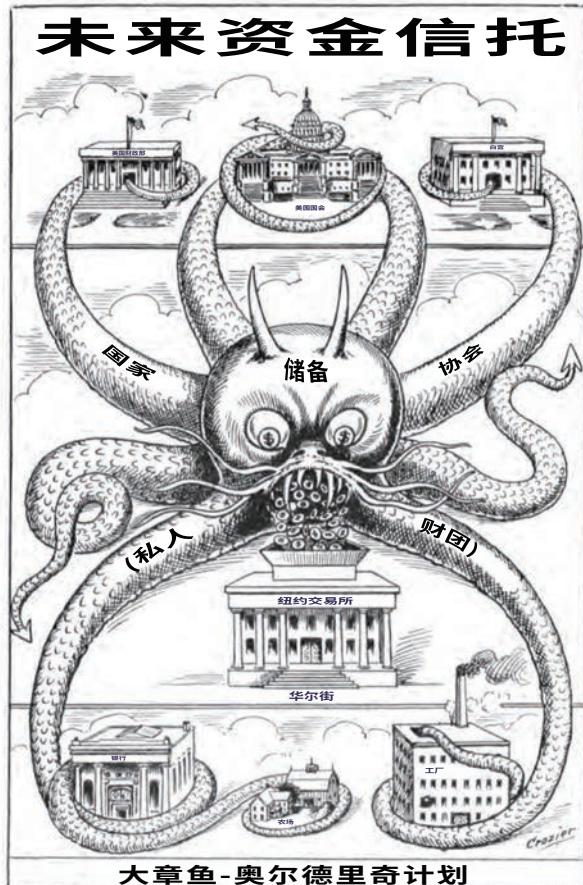
中央银行

中央银行是幕后操纵者，理应控制货币供应量的增长。但问题是，中央银行也受制于政府的法律，为政府的利益服务——这就像一个木偶人被另一个木偶人控制。中央银行看似是掌权者，其实是间接地在为政府服务，并在政府需要的时候凭空印钞。

他们如何受益

这些集团以各种方式获益，就此形成了一个复杂的控制网络。政府获得资金而不会立即产生后果，富裕的个人和银行毫不费力地赚钱，中央银行则维持着这场“演出”。与此同时，其他人群可能会感受到影响，并随着系统的发展而面临挑战。

最终，法币系统的傀儡们制造了一场少数人受益匪浅，许多人却对自己所处的金融舞台的公平性感到怀疑的表演。





第四章

中央银行的作用

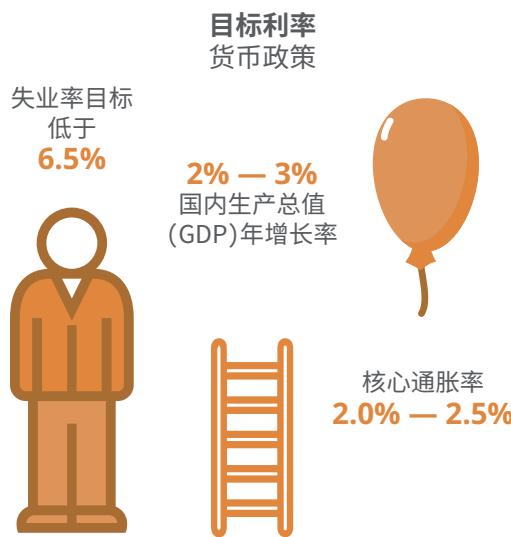
中央银行默默地影响着经济的运行。它们的官方职责是确保稳定性、诚信和“保持稳定”，但它们的方法揭示了更为神秘的一面。

中央银行与政府密切合作，操纵货币政策，利用利率等工具控制货币供应。在危机时期，它们会凭空印钞，并通过商业银行将钞票注入经济环境，从而让人觉得一切正常。

中央银行不只有看管的作用，它们还监管商业银行、制定规则，并在银行遇到困难时出手相助(充当最后贷款人)。这张控制网看似在保护银行，却让经济和银行更加依赖中央银行。

了解数万亿美元的刺激资金从何而来，以及谁能决定资金的分配，对于理解更为广泛的金融体系至关重要。各国政府在特定时刻可以使用多种工具来管理货币供应。

中央银行和政府可以使用货币和财政政策工具来影响货币供应和经济。例如，美国联邦储备局(美联储)利用货币政策来调整利率，进而影响流通中的货币量。另一方面，财政政策可以使用支出和税收政策来影响经济活动。



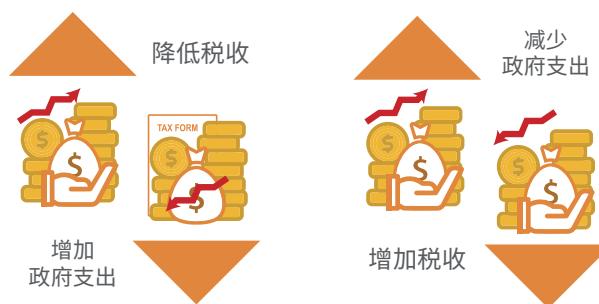
扩张性
财政政策

旨在增加消费者支出和企业投资，以提高总需求和经济增长。

VS

紧缩性
财政政策

旨在减少消费者支出和企业投资，以减缓不可持续的经济增长，并防止或降低高通胀。



什么是法定货币？ 法定货币由谁控制？

汇率政策、供应冲击和价格控制，是调节货币供应、影响贸易和经济的额外工具。虽然这些政策旨在稳定物价和控制通货膨胀，但干预往往会导致繁荣和萧条的循环，给使用受控货币的每个人带来挑战。

举例说明：“大而不能倒”是指因金融机构规模过大且相互关联，以至于其一旦倒闭，就会对整个金融体系造成灾难性的影响。2008年金融危机期间，几家大型银行被认为“大到不能倒闭”，故而美国政府选择对其进行干预并提供救助，以防止其倒闭。

在金融危机期间，雷曼兄弟控股公司是“大而不能倒”的机构中最为突出的例子之一。2008年9月，雷曼兄弟申请破产，引发了多米诺骨牌效应，其中包括保险巨头 AIG 濒临倒闭和股市大跌。于是美国政府不得不进行干预，向其他主要金融机构提供救助，以避免进一步的混乱，并保护更广泛的经济。

了解这些政策是如何运作的，对于理解中央集权式法定货币体系的局限性至关重要。如果不了解问题所在，就无法找到解决办法。既然我们已经介绍了法币系统在过去和现在是如何运作的，那么我们现在就来讨论一下法币的未来是什么样的：中央银行数字货币(CBDCs)。

4.3 中央银行数字货币：法定货币的未来

中央银行数字货币(CBDCs)是法定货币的下一步。与实体钞票、硬币和数字支付的组合不同，CBDCs是由政府发行并由中央银行控制的完全数字化形式的法定货币。

想象一下你每天都在使用货币，却没有任何实物存在——既没有硬币在你的口袋里叮当作响，也没有纸币需要折叠和展开。CBDCs的与众不同之处在于，它们为政府和中央银行提供了更高水平的控制和监测。有了CBDCs，当局在金融交易方面获得了前所未有的可见性，因而更容易跟踪和监管货币流通。

政府和中央银行可以随时调整CBDCs的形式和供应、操纵利率，并更精确地部署货币和财政政策工具。从本质上讲，CBDCs为当局影响和管理其法定货币提供了更有效的手段。

尽管CBDCs似乎是法定货币的未来，但当前世界的货币体系已经在按照纯粹的法定本位制运行了。法定货币不再与黄金挂钩，这导致货币供应量在没有任何实际限制的情况下大幅扩张。

现在，你对法定货币体系的运作方式有了更清晰的了解，是时候在第5章中探讨其后果了。

第五章

如何用问题 促成解决方案

5.0 问题简介

5.1 购买力下降

5.1.1 货币通胀及其对购买力的影响

活动: 通货膨胀的影响 - 拍卖活动

5.2 全球债务负担与社会不平等

5.2.1 对个人的影响 - 购买力的丧失

5.2.2 对社会的影响 - 财富不平等加剧

活动: 法定货币体系的后果

5.2.3 全球债务负担

5.3 密码朋克与去中心化货币的探索

5.3.1 密码朋克

5.3.2 集中化与去中心化系统

5.3.3 数字货币简史

如何用问题促成解决方案

5.0 问题简介

谁控制了我们国家的货币量，谁就是所有工商业的绝对主宰……当你意识到整个系统很容易就能被高层的少数权贵以这样或那样的方式控制时，你们不必被告知通货膨胀和萧条是如何产生的。

詹姆斯·加菲尔德，美国总统

在第4章中，你了解到金融世界所依赖的系统可能并不像看上去那么强大。由不断增加的纸币支撑的法币系统似乎只能让少数人受益，而不是多数人。本章揭示了法定货币体系对普通人和社会的意义。最后，我们将探究那些注意到了这些问题的人的故事，并默默地努力寻找可能改变人类社会未来的解决方案。

5.1 购买力下降

5.1.1 货币通胀及其对购买力的影响

货币通胀指一个经济体中货币供应量的增加，会直接影响普通人的购买力。当流通中的货币增加时，物价就开始了上涨的周期，而这反过来促进了人们对商品和服务的需求，并最终导致商品价格上涨。

让我们想象一下，亚历克斯、鲍勃和查理这几位朋友每个人手里都有一美元，以及一瓶水可供售卖。最初的情况很简单：这三个人一共有三美元和一瓶水。现在，假设当地政府决定给每个人多一块钱，那么他们此刻总共有六美元。有了这笔新的钱后，他们都想买一瓶水。由于三个人都想得到同一瓶水，于是他们开始互相竞价。

在额外的金钱的推动下，需求的增加导致他们的出价高于水瓶最初的价格。最后，竞价战导致水瓶价格上涨。这种情况反映了他们购买力的下降——即使他们有了更多的钱，也不能买到以前那么多瓶水，这显示了通货膨胀对货币的价值的影响。

在这个例子中，大家的购买力之所以下降，是因为他们使用的货币形式受到了外部因素的影响，比如政府增发的美元等。由于缺乏对货币供应量的控制，再加上需求增加导致物价上涨，使得朋友们即便是用多出的美元购买相同数量的商品，也会变得更具挑战性。

这说明了人们的购买力是如何受到他们无法控制的因素的影响的，强调了了解及质疑影响我们金钱价值的制度的重要性。

现在，就让我们来探讨一下在现实生活中是如何实现这一点的吧。



第五章



活动: 通货膨胀的影响 - 拍卖活动

目的：了解通货膨胀的概念及其是如何影响经济中商品和服务的价格的。

定义

 货币供应量：一个经济体在特定时间内流通的货币总量，主要包括以下内容。

- 实物货币，例如硬币和纸币等。
- 支票账户。
- 储蓄账户。
- 货币市场账户。
- 100,000 美元以下的小额定期存款。

 拍卖：将货物或财产进行公开拍卖，出售给出价最高者。

课堂练习 - 请按照以下说明进行练习

1. 你将从老师那里随机获得一定数量的垄断货币，这代表了一个社会的货币供应量。
2. 在提供给你的图表中写出货币供应总量。
3. 老师将向学生拍卖一块糖果。要想赢得糖果，你就需要用自己的垄断货币给出最高价。将中标价记录在图表上的货币供应旁。
4. 随后，教师将在货币供应总量中加入大量垄断货币，这代表一个经济体中货币供应量的增加。稍后，你们将学习该如何在一个经济体中增加或减少货币供应量。



社会总是难以预测和颇为不公正的，可以通过模拟一个老师随机将大量金钱分配给少数学生来体现这种情况，即模拟现实生活中资源和机会分配不平等的情况，这突出了社会在许多情况下固有的随机性和不公平性。

5. 老师将采用与之前相同的流程，向学生拍卖第二块糖果。将中标价记录在图表上的货币供应旁边。
6. 老师将重复第三次拍卖。

如何用问题促成解决方案

轮次	货币供应量	中标价
1		
2		
3		

结论

1. 货币供应量的增加对糖果的中标有什么影响?
2. 增加货币供应量与通货膨胀之间有什么关系?
3. 货币供应量与现实世界有何关联?
4. 你认为当把新货币注入经济时，商品和服务的价格会发生什么变化？你觉得价格的变化是暂时的还是永久的？为什么？从长远的角度来看，你认为物价变化会对社会中的公民产生什么影响？

5.2 全球债务负担与社会不平等

5.2.1 对个人的影响 - 购买力的丧失

詹姆是一名住在一间小公寓里的大学生。他现在通过在一家咖啡店打零工来支付自己的生活费和学费。詹姆一开始独立生活，便开始妥善地管理自己的账簿。



账簿详细地记录了你所有的货币交易。无论是收入还是支出，都应被记录在账簿上。

2023年初，詹姆为自己全年的生活费用(包括房租、食品和其他必需品)做了预算了，为10,000美元。以下为詹姆在2023年1月的交易情况。



第五章

日期	说明	金额(美元)	类型	余额(美元)
01/01/2023	起始余额			1,600
01/01/2023	一月份租金	800	支出	800
01/05/2023	杂货	100	支出	700
01/15/2023	兼职工资	500	收入	1,200
01/20/2023	汽车汽油	350	支出	850
01/30/2023	教科书	150	支出	700

这本账簿显示，詹姆的起始余额为1,600美元，其中800美元用于支付当月房租(借方)。然后，詹姆花了100.00美元购买日用品，并收到了500美元的兼职工资(贷方)，此时余额达到1,200美元。然后，他又花钱买了汽油和教科书。截至月底，詹姆的余额降到了700美元。

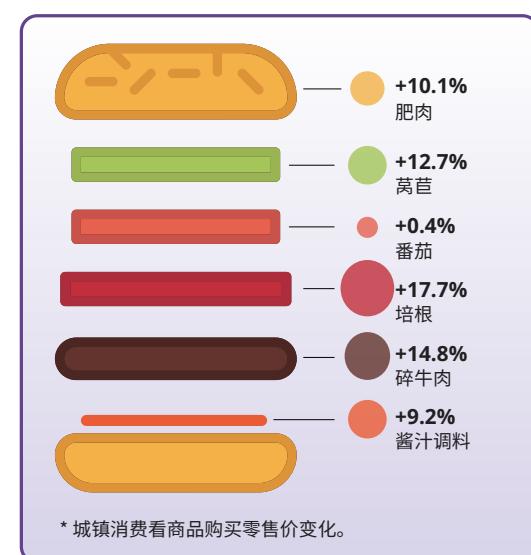
12个月后，詹姆与祖父共进午餐，并与祖父分享了他在2024年的预算细节。詹姆注意到，他的预算不像以前那么宽裕了，因为他的生活费用在过去一年大幅增加。正当詹姆为此感到疑惑时，他的祖父向他展示了右边的图片。

詹姆简直不敢相信自己的眼睛——他猛然发现，商品和服务的成本一直在随着时间的推移急剧增加，这导致他的购买力不断下降。

詹姆的祖父说：“1956年的时候，我还是一个初出茅庐的年轻人。我记得当时我在工厂当工人，每月能挣380美元。这看起来似乎并不多，但在当时已是一份体面的工资。事实上，我当时已经攒够了可以在郊区给自己买房子的钱。”

祖父继续道：“20世纪的物价与现在大不相同。例如，在2020年，购买30块好时巧克力需要花费26.14美元。然而，如果我们回到1913年，购买同样数量的好时巧克力只需花费1美元。”

这种价格上的巨大差异凸显了购买力随时间推移而发生的变化，也体现了购买力是如何随着通货膨胀而变化的。

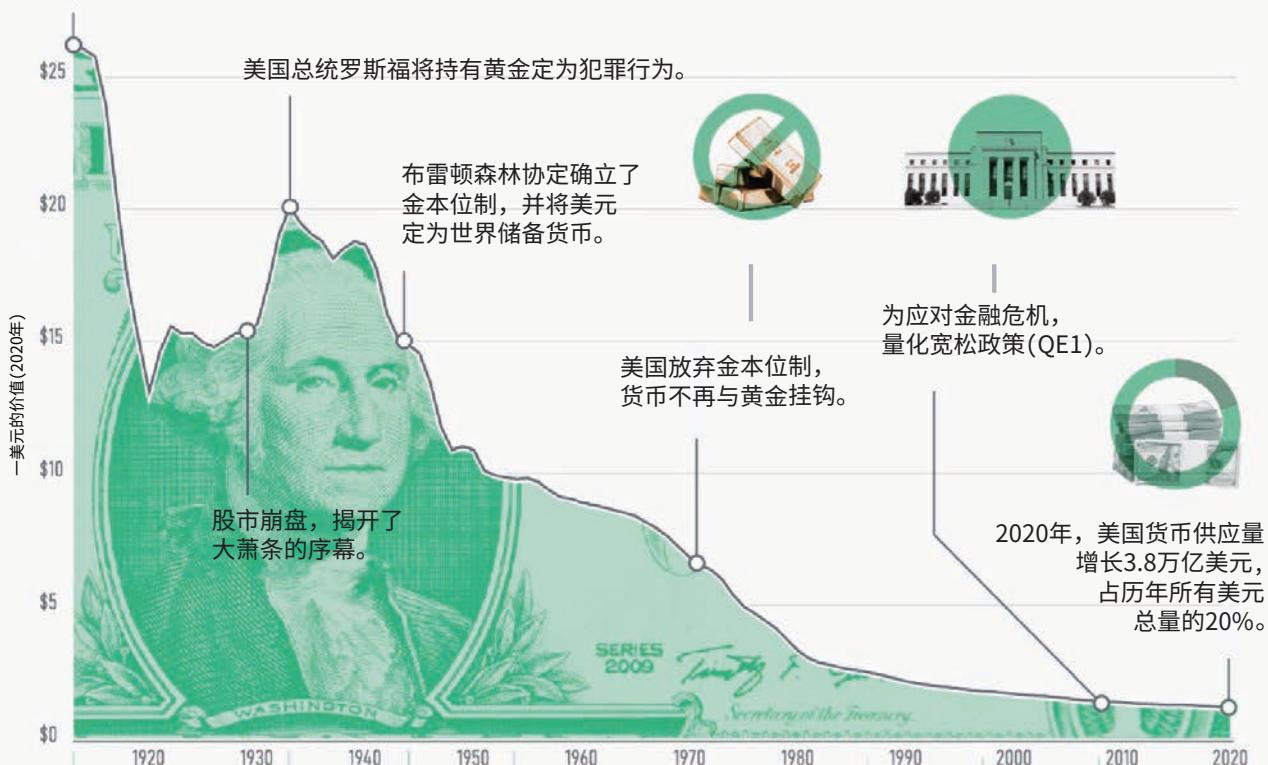


如何用问题促成解决方案

美元的价值 美元购买力

由于通货膨胀和货币供应的增加，
美元的购买力在过去一个世纪里大幅下降。

《联邦储备法案》创建了一个能够管理国家货币供应的中央银行。



1美元的购买力(按2020年美元计算)



詹姆：“什么？这太疯狂了。我无法想象如果在那时租房，我的房租会比现在低多少。”

爷爷：“嗯，是的，你的房租的确会便宜得多。我这里还有一个例子可以说明这一点：1美元在那时可以买到大约10袋椒盐脆饼。但在2020年，我花了9.69美元才买到同样的数量的椒盐脆饼。想象一下，10袋椒盐脆饼在今天值多少钱。”



第五章



詹姆：“哇，爷爷，这真的很有趣。你年轻的时候是如何经历这一切的？”

爷爷：“詹姆，我年轻的时候所有东西都要便宜得多。那时候一条面包只要0.18美元，一加仑汽油只要0.29美元。现在生活成本涨了这么多，真是让人难以置信。”

在与祖父谈话后，詹姆回到家又看了看自己的账本。他很快发现，自己需要在2024年的预算中增加1,000美元，才能购买与上一年相同的一篮子商品和服务——这意味着他的购买力下降了1,000美元，因为他现在必须花更多的钱才能买到同样的商品和服务！詹姆的工资只是略有增加，他的生活成本却在逐年飙升。

下表显示了詹姆第一年和第二年的支出以及价格上涨的百分比。

为了能继续生存下去，詹姆每周都需要工作更多时间，从而获得额外的1,000美元，使其能够维持与上一年相同的生活标准。

根据美国劳工统计局提供的信息，美国现在的物价大约是1913年的30倍。这意味着现在的1美元，只能买到当时的1美元能买到的东西的3%左右。

项目	第一年的花费	第二年的花费	增幅百分比
租金	\$4,000	\$4,500	12.5%
杂货	\$2,000	\$2,300	15%
必需品	\$4,000	\$4,200	5%
总计	\$10,000	\$11,000	10%

例如，假如有人给詹姆提供了一个穿越时空的选择——要么拿走1913年的100美元，要么等到2023年只得到3美元——这就好比在过去疯狂购物和在今天只得到一些小点心之间做出选择。价值上的巨大差异充分表明货币的购买力在这些年来究竟下降了多少。

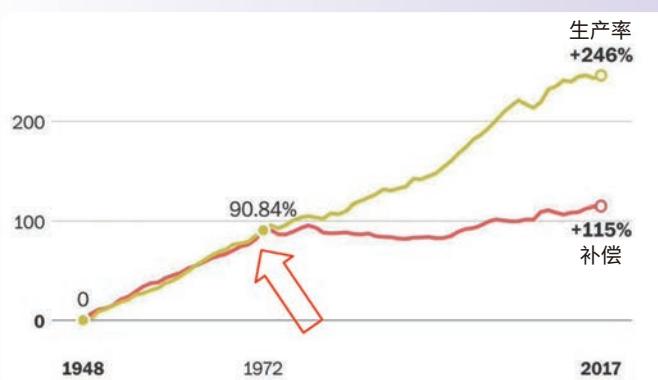
1938的生活成本	
<u>生活支出</u>	
新房子	\$3,900.00
平均收入	\$1,731.00/年
新车	\$860.00
平均租金	\$27.00/月
哈佛大学学费	\$420.00/年
电影票	25¢/张
汽油	10¢/加仑
美国邮票	3¢/张
<u>食物支出</u>	
白砂糖	59¢/10磅
含维生素D的牛奶	50¢/加仑
研磨咖啡	39¢/磅
培根	32¢/磅
鸡蛋	18¢/打

(根据原图)

如何用问题促成解决方案

从数字上看，詹姆一年赚的钱比他祖父要多得多，但詹姆祖父当时拥有的美元在那个时候比现在要值钱得多，能购买的东西也多得多。

生产率和每小时补偿的增长 (1948—2017)



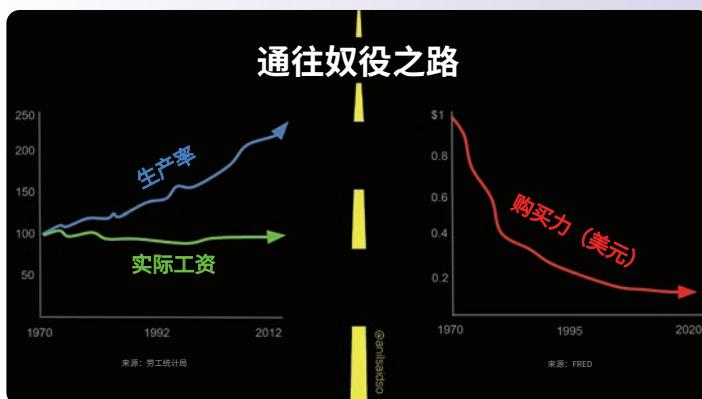
注：补偿包括生产和非监督岗位工人的工资及福利。

在当今世界，通货膨胀所造成的影响使得人们不愿意存钱。

与之相反的是，大多数人选择立即花钱，因为钱会迅速贬值。这种对前景的悲观对他们规划未来的能力产生了阻碍。

如上图所示，在根据通货膨胀进行调整后，普通人的工资仍然停滞不前，这意味着尽管他们工作得更加努力，但他们的加薪速度远远赶不上货币的贬值速度。

詹姆的例子只是众多例子中的一个。在货币世界里，政府为了推行自己的计划而凭空创造货币是司空见惯的事情，后果却要全世界的个人来承担。从面包到住房，从日用品到节假日，日常用品的价格每年都在上涨。富人因拥有资产而从通货膨胀中受益，普通人却只能眼睁睁地看着自己辛苦赚来的钱再贬值。结果是什么？世界各地的人们和家庭纷纷因购买力下降而陷入困境。



世界各地的人们纷纷发现，为了维持同样的生活水平，他们需要做更多的工作，花费更长的时间。这就像在跑步机上跑步，尽管跑得越来越快，却永远无法真正出人头地。货币体系让人们感觉自己似乎永远都在与不断上涨的物价赛跑。



第五章



许多人在努力追赶日益增长的成本时不得不举债度日，而这不过是杯水车薪。人们之所以选择贷款或做出冲动的决定，只是为了勉强度日。至此快钱成为一种必需品，人们发现自己陷入了一种循环——今天的生存优先于明天的规划。

可以不断印钞的法定货币体系影响着人类的心理。它向人们灌输了一种高度的时间偏好——注重短期收益而非长期规划。这无疑是一种急功近利，法币世界中的个人往往倾向于优先考虑短期利益。这是一种生存本能，它导致了一种依赖循环，即个人会寻求任何手段来获得快钱，即使这种手段从长远来看是不可持续的，甚至是行不通的。

从本质上讲，货币体系的影响为全球的个人描绘了一幅充满挑战的图景。在货币体系中，物价上涨、收入停滞，为生存而挣扎成了人们每天都在进行的战斗。虽然某些群体变得更加富有，但全球大多数人仍然不得不依赖一个让他们越来越穷的系统。

5.2.2 对社会的影响 - 财富不平等加剧

在一个以稳健货币为基础的社会中，政府的财政决策通常需要获得人民的支持与认可。然而，在法定货币体系下，政府可以依靠公民背负债务的方式，积累几乎无限的债务。随意印制货币的权力常常会导致政治权力的集中。法定货币体系使得政府能够累积巨额债务，做出有利于自身而非大众的决策。像美国这样的超级大国就凭借这种现象获得了竞争优势，它们可以不受限制地印制货币，用以资助自己的各种计划，包括战争。这一能力使这些国家能够控制、影响，甚至参与地缘政治冲突，进而导致全球权力失衡。对于这些超级大国来说，发动战争和采取重大控制他国的行动在财政上变得可行，那些没有相同的财政灵活性的国家则会面临诸多限制。

在法定货币体系下，财富不会平等分配。相反，财富往往会集中在少数人手中。这就像在玩大富翁游戏，只有少数玩家拥有几乎所有酒店和地产，大部分玩家则要为生存而挣扎。法定货币体系已经变成某些团体集中财富的工具。通过印钞，政府与中央银行密切合作，将更多货币注入经济，而这些新创的货币会首先流入那些拥有既得财富和地位的强大实体和个人手中。这些团体能够在新印制的货币尚未开始对经济产生购买力下降等负面影响时，提前从中获利。

如何用问题促成解决方案

财富不平等不只是富人和穷人的问题，更是压制经济流动性的问题。那些出身不那么优越的人发现，在经济阶梯上攀登变得越来越具有挑战性，就像背负着沉重的背包开始比赛一样。贫富差距的不断扩大给每个人都带来了问题——富人制定了对他们有利的政策，这让普通人的生活变得更加艰难，甚至导致社会动荡，人们对机构缺乏信任，社区分崩离析，就像纸牌屋一样。当西方世界面临经济衰退时，法币体系的不稳定性表现为经济不确定性、政治动荡，以及全球影响。

这是一种全球现象，对发达国家和发展中国家的社会均会产生影响。富裕阶层往往会选择跨国经营，利用全球金融体系为自己谋利，从而进一步拉大上层与下层之间的差距。

在法定货币体系下，负债已成为人类的常态。全世界的政府、机构、企业和个人都发现自己正沉浸在债务的海洋中。将债务视为可以接受的心理转变，源于法定货币体系的设计。在过去的几十年里，实体越来越容易背负巨额债务；而对于普通人来说，由于物价和生活成本的上涨，债务也成了一种必需品。

消费主义是一种持续不断的购买和消费冲动，它会导致人们购买超过自己需要的东西，以致过度消费和浪费。虽然这看起来像一场永无止境的购物狂欢，但其真正的代价不只在于价格，而是会影响人们的心理和健康。

由此可见，货币体系不仅是一种经济机制，还是一个塑造整个人类社会的体系。从权力集中到全球动态、贫富差距和社会规范，货币体系直接影响着国家的运作方式和普通公民的生活方式。



活动: 法定货币体系的后果

1. 在经历了法定货币体系之后，个人和整个社会还会有什么后果吗？
2. 在你的国家，法定货币制度会带来什么后果？历史上发生了什么？对你的国家的人民产生了什么影响？
 - a. 个人实例——互动环节

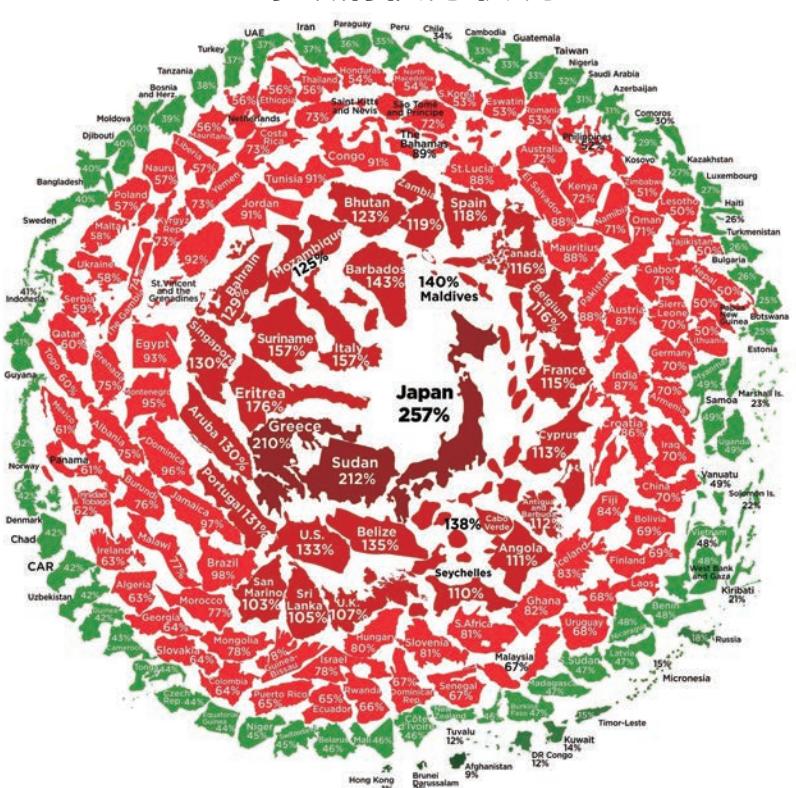
5.2.3 全球债务负担

由于法定货币体系，各国政府均发现自己陷入了一个巨大的债务网，陷入了所谓的“全球债务螺旋”。试想一下，你借的钱多到永远无法偿还，而这种情况正在全球大规模发生。被债务淹没的各国政府陷入了一场危险的游戏，其积累的债务远远超过了他们所能偿还的数额——这是一个不计后果的消费、借贷和短视的故事，如今正将世界各国推向金融灾难的边缘。



截至目前，美国联邦政府自2019年以来新增的债务已达到惊人的10万亿美元。债务总额已从2019年第四季度的约23万亿美元，飙升至如今的34万亿美元的天文数字。事实上，全球各国政府债务增长的速度不仅没有放缓，甚至还在加快。预计2023年将会是自2021年“新冠”时期以来，债务增加最多的一年。

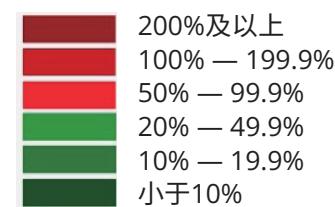
全球政府债务状况



那么，这对已经需要应对法定货币体系后果的个人和社会意味着什么呢？他们陷入的债务漩涡就像从山上滚下的雪球，越滚越大，而我们却不知道如何阻止它。

前面提到的后果，从财富不平等到社会动荡，都不会消失。相反，全球债务负担已经到了无法挽回的地步，让事情注定会变得更糟。

2021年债务占GDP比例 (%)

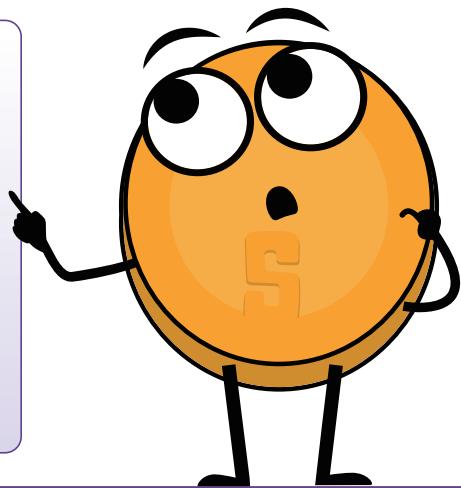


如何用问题促成解决方案

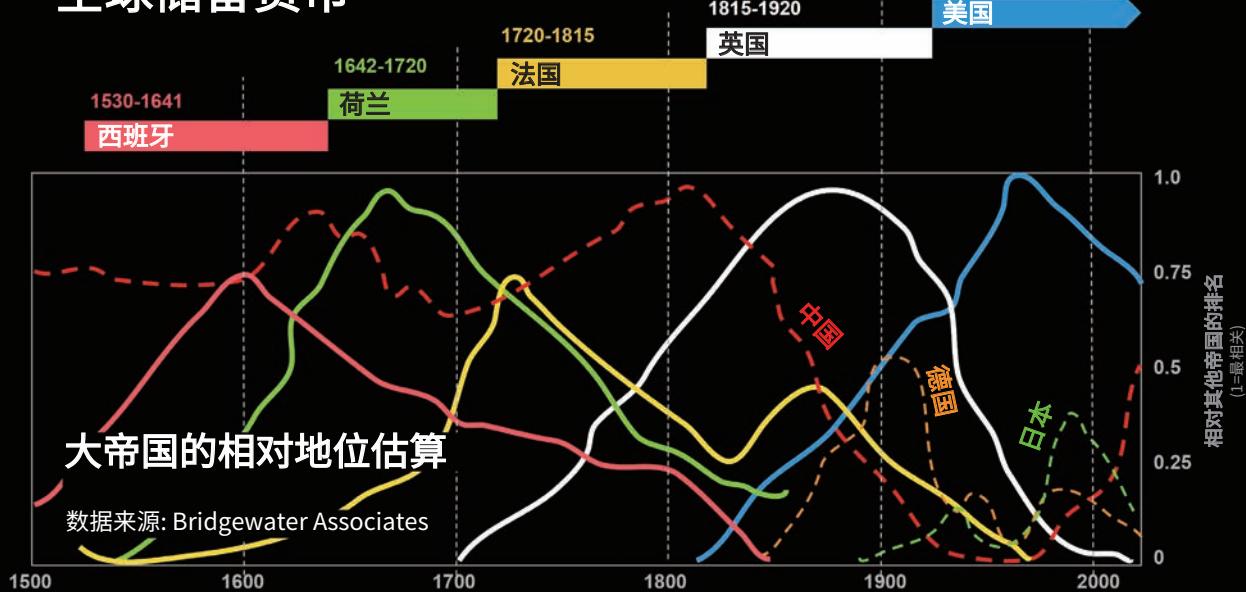


我不认为我们能再次拥有良好的货币，除非我们能将货币从政府手中剥离……我们所能做的，就是通过一些巧妙而间接的方式，引入一种他们无法阻止的东西。

弗里德里希·哈耶克
诺贝尔经济学奖获得者



全球储备货币



5.3 密码朋克与去中心化货币的探索

在整个历史中，银行和政府逐步攫取货币，并最终形成了我们今天所熟知的法定货币体系，给社会带来了灾难性后果。但加密技术和互联网等新技术的兴起让新的想法得以出现，比如独立的数字货币。数字货币不受政府干预、向所有人开放，并且所有人都可以使用。让我们深入了解领导这场革命运动的“密码朋克”的历程吧。



第五章



5.3.1 密码朋克

可以将计算机作为解放和保护人民的工具，而不是控制人民的工具。

哈尔·芬尼

20世纪下半叶，计算机和互联网等多项技术突破的兴起为全新的数字时代铺平了道路。

一部分人发现，这些大规模的创新将很快改变社会的运行方式。他们预见了个人电脑的潜力和危险——它既可以成为赋予个人自由的工具，也可以成为完全控制和监视个人的工具。

这些人被称为“密码朋克”。他们是一个由活动家、密码学家、程序员和隐私保护积极分子组成的松散团体，有着共同的愿景：追求隐私、安全和去中心化的数字未来。密码朋克，也就是“Cypherpunk”一词，融合了“cypher”和“punk”，“cypher”指的是密码，而“punk”代表反叛文化的精神。

密码朋克相信密码学能够保护个人自由。他们的目标包括开发能确保在线通信安全的工具、匿名互联网活动，以及建立不受中央机构控制的数字货币。

密码朋克明白法定货币体系的后果，也看到了“奥威尔式未来”的威胁。他们认为，必须确保个人电脑和互联网成为人类的福祉，而非加剧国家对人民的控制的工具。



奥威尔式未来的定义

奥威尔式未来指受乔治·奥威尔的作品启发而产生的一种乌托邦式的愿景。这个词与噩梦般的极权社会有关，其特点是政府高压控制、广泛监视、宣传和操纵信息。“奥威尔式”一词通常用于描述这样一种情景：公民的自由和个人自主权受到严重限制，不同政见受到压制，现实被扭曲，以满足强大的专制政权的利益。这个概念是以乔治·奥威尔的名字命名的，他在自己的著作中对不受制约的政府权力和基本人权受到侵蚀的潜在危险提出了警告。

如何用问题促成解决方案

密码朋克运动的主要人物包括埃里克·休斯、蒂莫西·C·梅和约翰·吉尔摩等知名人士。1992年，埃里克·休斯撰写了《密码朋克宣言》，概述了该组织的原则。宣言强调了隐私、加密的重要性，以及个人控制数字身份的必要性。

密码朋克最著名的发明之一，便是创建加密工具和协议。1991年，菲尔·齐默尔曼(Phil Zimmermann)推出了电子邮件加密软件PGP(Pretty Good Privacy)，它随后成了一个旗舰项目。PGP允许用户在互联网上发送加密信息，除收件人外，任何人都无法解密该信息。在此之前，任何通过互联网发送的信息都有可能被他人(比如政府)截获和读取。

密码朋克认为，加密技术的突破以及互联网和计算机的出现，为在数字空间创建去中心化网络提供了坚实的基础，使个人可以在互联网上进行私下交流与交易，而不必受中央机构干扰。

密码朋克走上了正确的道路，为人类创造了一个更加光明的未来。在这个未来里，技术将成为最大化的自由而非控制他人的工具。而唯一缺少的，就是去中心化网络和去中心化数字货币。



观看此视频，
了解密码朋克
的故事！

5.3.2 集中化与去中心化系统

中心化系统：一个统治者，许多问题

在中心化系统中，一切都围绕着一个像城市中的高楼大厦一般的主要机构。正是这个机构控制着整个系统的运作。以传统银行为例，其所有决策都是由一个小团体做出的。

真实案例：2022年，在加拿大的和平抗议活动中，银行冻结了抗议者的账户，这表明中央权力机构可以介入甚至控制金融访问。





第五章

中心化的问题

- ◆ 中心点故障：如果中央机构出了问题，那么整个系统就会崩溃。
- ◆ 控制：高层的一小部分人拥有很大的控制权和权力，他们做出的决定往往比其他人更利己。
- ◆ 低效和中间商：就像城市里的交通堵塞一样，中心化系统会因为不必要的中间商而变得缓慢和昂贵。
- ◆ 缺乏自主权：人们可能无法自己做出财务选择，因为一切都由最高权力机构决定。
- ◆ 审查和限制：就像城市中的某些地方可以被封锁一样，中央系统也可以封锁或限制对某些金融资源的使用。
- ◆ 扩展面临挑战：当越来越多的人需要金融服务时，中心化系统可能会难以跟上。
- ◆ 安全风险：中央机构的问题会导致整个系统面临网络攻击的风险。
- ◆ 缺乏透明度和信任：由于人们难以了解中心化系统的内部运作，因此可能很难对其产生信任。

去中心化系统：权力属于人民

现在，把去中心化系统想象成一个大森林——每棵树都代表一个独立的部分，整个森林则代表整个系统。与只有一个中心点的城市不同，去中心化系统更像一个有弹性的森林，即使某个部分出现问题，它也能继续前进。

- ◆ 真实案例：Tor网络及其浏览器创建了一个去中心化系统，使人们可以在互联网上匿名，而且该网络很难被阻止或审查。



去中心化系统的好处

- ◆ 增强复原力和可靠性：即使存在一些问题，在没有单点故障的情况下，也能使系统变强。
- ◆ 提高安全性：有了正确的加密/保护措施，分散式系统就能更好地抵御单一机构的控制。

如何用问题促成解决方案

- 更大的主权：人们可以更多地控制自己的资金、数据和决策。
- 提高透明度：每个人都能看到相同的信息，从而提高系统的可信度。
- 无权限、无限制：任何人都可以加入或参与，使其成为一个包容性的金融体系。
- 机会均等：每个人都有公平的做出贡献和发表意见的机会。
- 增强隐私性：数据分布在多个参与者之间，而且大多是匿名的，因此分散式系统的隐私性更强。

虽然去中心化系统有很多优点，但在共同决策方面可能有点棘手，这就需要每个人齐心协力。

改变行使权力的方式

在集中式和分散式系统的世界里，权力掌握在谁手中至关重要。集中式系统将权力赋予一小部分人，分散式系统则将权力分散，让每个人都有发言权。这种权力的转移意味着一个更公平、更民主的金融未来，这让许多人都能影响并塑造他们所生活的系统。

5.3.3 数字货币简史

密码朋克所讨论的最关键的概念之一就是数字现金。密码朋克意识到，需要分离国家和货币，才能确保在未来能够造福大众。戴维·查姆 (David Chaum) 在加密协议方面的开创性工作为安全和私人交易奠定了基础。而不足之处在于，这种协议需要一个中央机构才能有效运作，这引发了对单点故障和潜在审查的担忧。

在随后几年里，多个密码朋克尝试对彼此的想法进行迭代，以创造一种不受政府控制的数字货币的可行解决方案。下表介绍了密码朋克在探索创建数字现金过程中的几项关键创新。

姓名和日期	说明	局限性
E-Cash (1982)	戴维·查姆的E-Cash是电子现金的早期概念，其重点是通过加密技术保护隐私	其需要一个中央管理机构，这引发了人们对单点故障和潜在审查的担忧
DigiCash (1990)	DigiCash由 David Chaum 创立，旨在创建一种注重隐私的数字货币形式	中央集权模式导致其最终于1998年破产。



第五章



B-Money (1996)	B-Money由Wei Dai提出，是一个匿名分布式电子现金系统的理论提案	该系统从未付诸实施，仍停留在概念上。
HashCash (1998)	由Adam Back开发的 HashCash 是一个工作证明系统，旨在限制垃圾邮件和拒绝服务攻击	没有直接解决与数字货币相关的双重消费问题
Bit Gold (1998)	尼克·萨博(Nick Szabo)提出的“比特黄金”描述了一种具有工作证明元素的去中心化数字货币系统	从未实施过，仍是一个理论概念
e-Gold (2004)	e-Gold是一种由实物黄金支持的中央数字货币，其允许用户购买和转移e-Gold单位	其因法律问题而于2009年关闭，这凸显了与中心化数字货币相关的挑战

尽管数十年来，密码朋克曾多次尝试创建一种不受任何团体或政府控制的数字货币，但他们的努力面临着实际挑战，因而无法在现实世界中完全实现。密码朋克们得出的结论是，要建立一种安全、可扩展、有可能被广泛采用的数字形式的现金并非易事。

然而，当一个人汲取了密码朋克的教训，将去中心化数字货币的概念提升到新的高度时，故事便发生了转折。在接下来的章节中，我们将探讨这个人是如何在之前40年的工作的基础上做出贡献，并最终创建了一个功能完善的系统的。

第六章

比特币简介

6.0 中本聪和比特币的诞生

6.1 比特币是如何运作的？

6.1.1 中本聪共识机制

6.1.2 游戏的参与者

活动: 在点对点网络中建立共识

6.2 作为稳健数字货币的比特币

6.2.1 引言

6.2.2 比特币的特性

活动: 课堂讨论 - 比特币是稳健货币吗？

6.2.3 承担个人责任

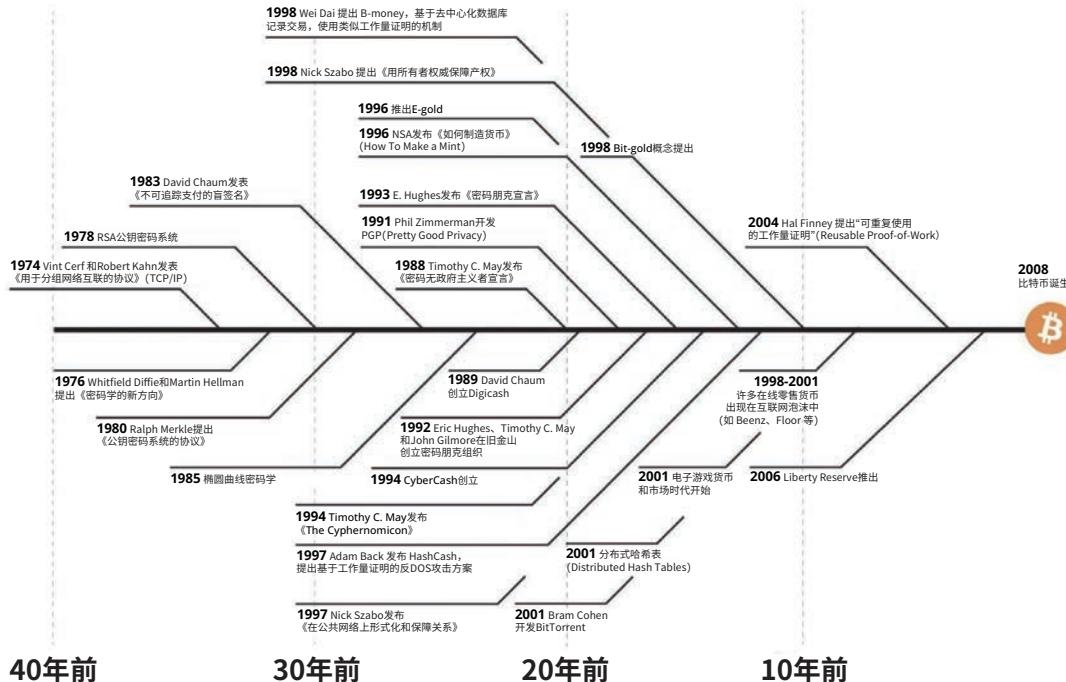
比特币简介

6.0 中本聪和比特币的诞生

许多人自动将电子货币视为一项失败的事业，因为自20世纪90年代以来，所有公司在这方面的尝试都失败了。但我希望大家明白，这只是电子货币的中心化控制性质造成的。这些制度注定了他们的命运。而我认为，这是我们第一次尝试一个分散的非信任系统。

中本聪

比特币的前史 - 历时40年的研究、开发与需求的成果



40年前

30年前

20年前

10年前

正如你在上一章中读到的，多个密码朋克曾试图创建另一种货币系统。本章将继续讲述其中一个人的故事：一个名叫“中本聪”的、有远见的人。在比特币出现之前，这个匿名者(男人、女人或团体)早已加入了计算机科学家和黑客等密码学爱好者的行列，并参与讨论以寻找替代法定货币系统的实用解决方案。

正如你在上一章中读到的，多个密码朋克曾试图创建另一种货币系统。本章将继续讲述其中一个人的故事：一个名叫“中本聪”的、有远见的人。在比特币出现之前，这个匿名者(男人、女人或团体)早已加入了计算机科学家和黑客等密码学爱好者的行列，并参与讨论以寻找替代法定货币系统的实用解决方案。

正如你在上一章中读到的，多个密码朋克曾试图创建另一种货币系统。本章将继续讲述其中一个人的故事：一个名叫“中本聪”的、有远见的人。在比特币出现之前，这个匿名者(男人、女人或团体)早已加入了计算机科学家和黑客等密码学爱好者的行列，并参与讨论以寻找替代法定货币系统的实用解决方案。

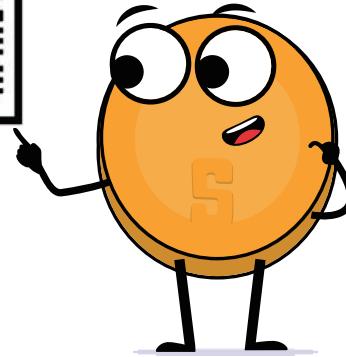
正如你在上一章中读到的，多个密码朋克曾试图创建另一种货币系统。本章将继续讲述其中一个人的故事：一个名叫“中本聪”的、有远见的人。在比特币出现之前，这个匿名者(男人、女人或团体)早已加入了计算机科学家和黑客等密码学爱好者的行列，并参与讨论以寻找替代法定货币系统的实用解决方案。

正如你在上一章中读到的，多个密码朋克曾试图创建另一种货币系统。本章将继续讲述其中一个人的故事：一个名叫“中本聪”的、有远见的人。在比特币出现之前，这个匿名者(男人、女人或团体)早已加入了计算机科学家和黑客等密码学爱好者的行列，并参与讨论以寻找替代法定货币系统的实用解决方案。



第六章

2008年10月，中本聪在一个密码学邮件列表上发布了一份开创性的白皮书《比特币：点对点电子现金系统》。这份文件为去中心化的点对点协议奠定了基础，旨在促进安全的在线交易，而无需中间商。中本聪的愿景很明确，摆脱强大的政府和金融机构的控制，创建一个纯粹的点对点版电子现金。



时间快进到2009年1月3日，中本聪挖出了第一个比特币区块，即“创世区块”。这标志着比特币网络正式启动，这是一个通过分散式分类账，建立在信任和安全的基础上的新货币系统。在随后的岁月里，越来越多的爱好者开始加入并为这一理念做出贡献。

比特币创世区块

原始十六进制版本

```

00000000 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000020 00 00 00 00 3B A3 ED FD 7A 7B 12 B2 7A C7 2C 3E
00000030 67 76 8F 61 7F C8 1B C3 88 8A 51 32 3A 9F B8 AA
00000040 4B 1B 5B 4A 29 AB 5F 49 FF FF 00 1D 1D AC 2B 7C
00000050 01 01 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00
00000060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000070 00 00 00 00 00 00 FF FF FF FF 4D 04 FF FF 00 1D
00000080 01 04 45 54 68 65 20 54 69 6D 65 73 20 30 33 2F
00000090 4A 61 6E 2F 32 30 30 39 20 43 68 61 6E 63 65 6C
000000A0 6C 6F 72 20 6F 6E 20 62 72 69 6E 6B 20 6F 66 20
000000B0 73 65 63 6F 6E 64 20 62 61 69 6C 6F 75 74 20 66
000000C0 6F 72 20 62 61 6E 6B 73 FF FF FF FF 01 00 F2 05
000000D0 2A 01 00 00 00 43 41 04 67 8A FD B0 FE 55 48 27
000000E0 19 67 F1 A6 71 30 B7 10 5C D6 A8 28 E0 39 09 A6
000000F0 79 62 E0 EA 1F 61 DE B6 49 F6 BC 3F 4C EF 38 C4
00000100 F3 55 04 E5 1B C1 12 DE 5C 38 4D F7 BA 08 8D 57
00000110 8A 4C 70 2B 6B F1 1D 5F AC 00 00 00 00 00 00 00 00

```

*图中文字：《泰晤士报》2009年1月3日，财政大臣正处于实施第二轮银行紧急援助的边缘。

2011年，在比特币网络证明了其无需有影响力的创建者也能成功运行之后，中本聪向一位比特币开发者同行发送了一封电子邮件，宣布自己将退出比特币舞台，并将比特币的未来交给与他有共同愿景的其他“好手”。

虽然中本聪的身份至今仍是一个谜，但他创建比特币的目标从来不是谜。从本质上讲，中本聪之所以创造比特币，是为了将权力从少数人手中夺走，还给大多数人，通过创造一种去中心化、开源和透明的货币系统，将货币与国家分离。2008年的金融危机伤害了全世界的普通人，却让精英阶层再次富裕。比特币是中本聪对法定货币体系的腐败和脆弱性的回应。中本聪为一场新的革命奠定了基础，但他并未居功自傲，而是选择了置身事外。

比特币简介

在随后的几年里，比特币开始迅速发展，并成为希望、赋权和韧性的象征。它挑战了法币系统，为人们提供了一种安全、抗审查的金融交易手段。比特币是一个开源协议，这意味着没有人有权拥有或控制它。比特币的设计是公开的，任何人都可以参与。

如今，中本聪关于无国界、透明和安全的金融系统的梦想仍在继续，并推动着我们今天所见证的自由化变革。每天都有普通人在选择退出法币系统，选择进入比特币世界。比特币中心——所谓的比特币循环经济——已经由世界各地的自由爱好者发起。甚至像萨尔瓦多这样正在寻找另一条道路的国家，也开始以自己的方式用起了比特币。

6.1 比特币是如何运作的？

6.1.1 中本聪共识机制

那么比特币是如何运作的呢？比特币功能繁多，就像无底洞一样。幸运的是，如果你是第一次进入比特币世界，那么你并不需要完全了解其工作原理就可以开始使用它。

使用互联网也是如此。大多数人都不知道 TCP/IP 协议是如何工作的，但他们每天都会发送电子邮件、信息，并在社交媒体上发布内容。开车也是如此。大多数人并不清楚汽车的工作原理，但他们开起车来依然得心应手。



然而，比特币仍然是一项相当新的技术，就像20世纪90年代的互联网一样并且尚未被广泛采用。因此，用一种简单的、技术含量较低的方式来掌握比特币的基础知识对我们来说是很有帮助的。



第六章

My
First
Bitcoin

HCM®

比特币运作背后的关键理念可以浓缩为一句话：比特币是人们在网上达成的协议。你可以把比特币想象成和朋友一起玩棋盘游戏。当你玩大富翁这样的棋盘游戏时，与其他玩家就特定规则达成一致，而大富翁游戏的规则之一是只接受特殊的“大富翁钞票”。如果詹姆斯(玩家之一)违反规则，用卫生纸代替“大富翁钞票”买房子，其他玩家就会告诉詹姆斯他是个骗子，并干脆不和他玩了。简而言之，要玩这个游戏，你们就必须就一套规则达成共识，而且不能偏离这些规则，否则就会被拒绝。

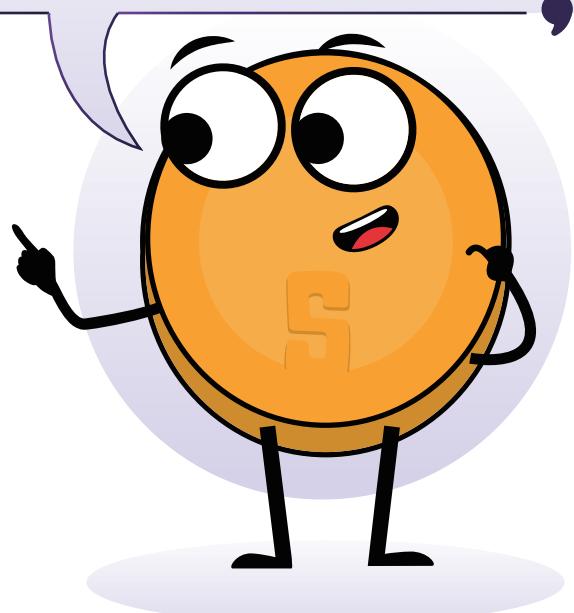
比特币就是这样运作的。比特币是一个由同意同一套规则的人组成的网络。这些规则以数学方式进行约束，用计算机代码进行编写，并被所有运行比特币软件的人接受。比特币的规则对所有参与者一视同仁，这意味着每个人要么遵守游戏规则，要么根本无法参与游戏，因为他们会直接被网络拒绝。

例如，规则之一是“比特币永远不会超过 2100 万枚”。如果有人想为自己多创造 100 万个比特币，那么这对他们来说毫无用处，因为他们会被其他人自动识别并拒绝。这就是比特币的强大之处——不管你是谁，也不管你来自哪里，只要你进入了比特币世界，就必须和其他人遵守同样的规则。这也适用于所有在法定货币世界中拥有巨大控制权和影响力的人和实体。在比特币的世界里，没有欺骗和破坏的空间，每个人都被平等地对待，没有人可以对此做任何事情。

你知道吗？自 2009 年以来，比特币已经经受住了数以万计的黑客攻击、篡改或更改它的尝试。比特币用事实证明了没有人能阻止、控制或操纵它。

“无论你是谁，无论你来自哪里，一旦进入比特币的世界，你就必须遵守与其他人相同的规则。”

这同样适用于那些在法币世界中拥有巨大控制力和影响力的人和个人机构。在比特币的世界里，没有作弊或破坏的空间——所有人一视同仁，这无可更改。



比特币简介

6.1.2 游戏的参与者

为了更好地理解比特币的去中心化，我们需要深入了解网络中的不同角色。在比特币世界中，不同的参与者扮演着不同但彼此和谐的角色，共同为网络的无缝运行做出贡献。

1. 矿工：安全建筑师

矿工是比特币的中坚力量。这些人或群体在幕后工作，通过一种叫做工作证明（PoW）的机制来维护和保障网络的安全。这些玩家配备了具有强大的计算能力的特殊的计算机。他们将自己的硬件提供给比特币网络，相互竞争以寻找复杂的加密数字、验证交易，并将新的交易信息块添加到比特币的分散式分类账（即所谓的区块链）中。他们的承诺确保了账本的不变性，并能防止恶意攻击。

挖矿的分散性使得任何拥有足够计算资源的人都能参与其中。由于他们的辛勤工作，最快解开谜题的矿工可以以比特币的形式获得奖励。

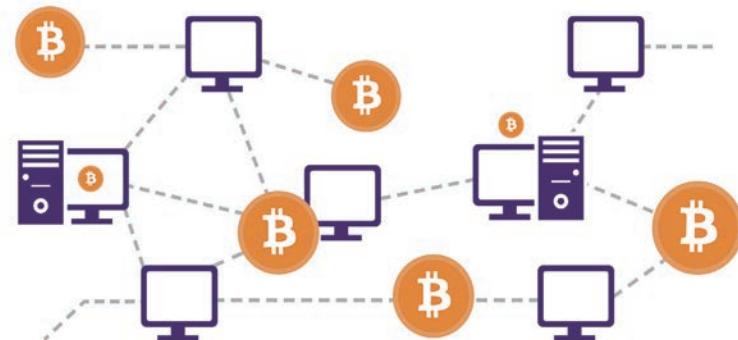
比特币矿工分布在世界各地，以保护网络不受集中化影响，同时确保比特币的安全性能保持稳健和分布式。



2. 节点：验证的守门人

比特币节点是生活在地球上的普通人。这些参与者在自己的小型计算机上运行比特币软件，维护整个分类账的副本，从而成为比特币网络的守门人。节点可以验证交易并确保所有参与者遵守共识规则。

通过在节点网络中分配验证责任，从而比特币可以抵御攻击，并保持其不可信的特性。节点在维护分类账的完整性方面发挥着至关重要的作用，为比特币的去中心化精神做出了贡献。





第六章



3. 用户：有能力的参与者

用户是比特币网络的生命线，是参与交易的个人。你可以把用户看作普通人，虽然他们只是过着自己的生活，但也通过某种方式融入了比特币，以增强自己的能力。例如，一些用户用比特币存钱；还有一些人，比如萨尔瓦多公民，用比特币购买日用品，并以工资的形式领取比特币。

比特币无需银行和政府等中介机构，允许点对点直接交易，用户的权能得以增强。这也意味着用户可以完全掌握自己的资金，同时对资金和交易进行控制。

4. 开发商和项目：创新建筑师

未来的货币体系既不会自行建立，也不会不费吹灰之力就以符合道德规范的方式被全球采用。而这就是比特币开发者和比特币项目发挥作用的地方。

开发者利用他们的技术专长来改进和创新比特币协议。他们贡献代码、提出改进建议、解决漏洞问题，以确保网络能够在应对各种挑战中不断发展。比特币的开源特性鼓励合作，从而让全世界的开发者都能为比特币的发展做出贡献。

这种去中心化的开发模式的好处在于防止单一实体垄断协议的控制权，这需要通过一个共识驱动的过程才能实现。开发者提出想法和改变，只有那些拥有最好的想法，并且与更广阔的美好世界愿景相一致的人，才能得到社区的支持，从而使比特币实现透明、民主的发展，直到其为 80 亿人做好准备。

比特币项目涉及各种不同团体，从有使命感的非营利组织，到公司，再到创造有价值内容的团体和个人，以及其他团体。这些人共同致力于实现比特币集体自由的大使命中的一个特定目标或重点。

比特币项目在塑造和促进比特币的应用方面发挥着至关重要的作用，它们致力于创造一个优先考虑人类赋权和自由的未来。

交响乐

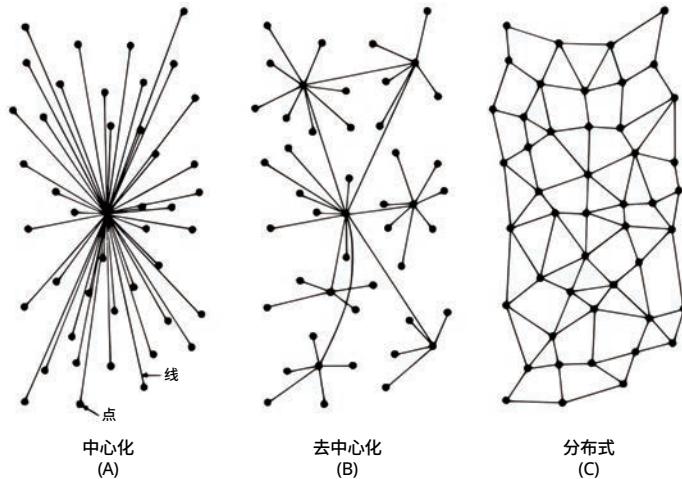
比特币的去中心化可以被看作一个协同作用的交响乐团，是让所有不同乐器演奏者共同演奏最美妙的音乐的平衡之举。在比特币网络中，没有老板，矿工、节点、用户、开发者和项目都在自主和协作中履行着自己的职责。

由节点维护的去中心化分类账保证了透明度，而工作证明机制提供了安全性，并阻止了挖矿的中心化。用户体验到金融主权和赋权，摆脱了法定系统的控制。开发者以共识为指导，确保协议能适应人类不断发展的需求。比特币项目以其独特的方式为集体自由这一更为广泛的使命做出了贡献。

正如你看到的，每个参与者都在塑造比特币的应用和增强人类能力方面发挥着至关重要的作用。在这个去中心化的乐团中，每一个参与者都为比特币的复原力和持久性做出了贡献，共同创造了一个无信任、无边界和赋权的生态系统。

比特币简介

总之，比特币的去中心化交响曲证明了中本聪的远见卓识和全球社区追求自由和赋权的巨大热情。



课堂练习 - 在点对点网络中建立共识



目的

了解该如何在群体中达成共识，学习密码学和比特币的共识层。



材料

带有加密和非加密行动指令(“攻击”或“不攻击”)的信息。



活动准备

教师将在课前挑选 3 或 4 名学生组成一个小组，使其在下面的活动中担任恶意节点。
教师将在上一堂课上给这些恶意节点布置一个密码谜题作为家庭作业。



第六章



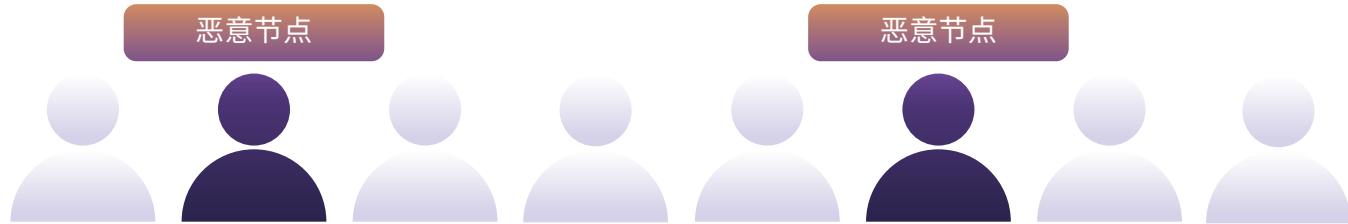
锻炼步骤



教师将选出一名“发起人”，他将收到写在纸上的信息“ATTACK(攻击)”，并将一串数字“4-16-14-21-1-21-21-1-3-11-”发给小组中的一名学生。



学生们将在指定空间内围成一个圈，以确保被选中的恶意节点学生被分开，从而提高课程效果。



小组围成一个圈后，发起人将纸条传给圈右边的人。



在每个人都读完信息后，发起人将向小组发出信号，说：“现在。”小组将同时对信息做出反应。如果信息是“攻击”，那么所有参与者都将向前迈出一步。



初步反应之后，一些学生（接收到加密信息并能正确解读的学生）会保持不动，其他学生则会按照原来的指令行事，这表明大家并没有达成共识。

结论

讨论未能达成共识的原因，介绍拜占庭将军问题的概念以及它与需要共同目标的关系，随后讨论比特币该如何为这一问题提供解决方案。

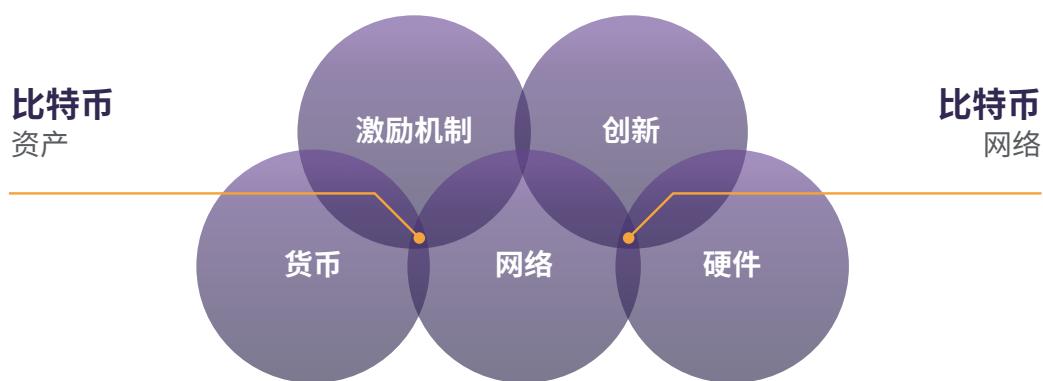
比特币简介

6.2 作为稳健数字货币的比特币

6.2.1 引言



简单地说，比特币就是钱。比特币不是一种投资，而是一种安全、高效的储蓄方式。拥有比特币并不意味着你会变得富有，因为它并不会给你带来更多比特币作为回报。以法定货币进行衡量的话，比特币的价值确实会上升，但这只是因为比特币的应用越来越广泛，以及法定货币的贬值。



比特币是一种新的货币形式，它是“货币互联网”。这意味着比特币是开放的，任何人都可以加入，并且已经开始与其他比特币用户进行价值交换。即使是世界上最偏僻、最贫穷的社区，也终于可以使用货币系统了。就像每个拥有手机和互联网连接的人都能使用搜索引擎一样，比特币让每个拥有手机和互联网连接的人都能使用新的全球货币系统。



几分钟内便可将资金汇至全球各地，且手续费极低。



25亿未享受银行服务的人群可以通过手机或电脑获得资金使用权。



虽然比特币交易是公开的，但您的身份不会被披露。



第六章

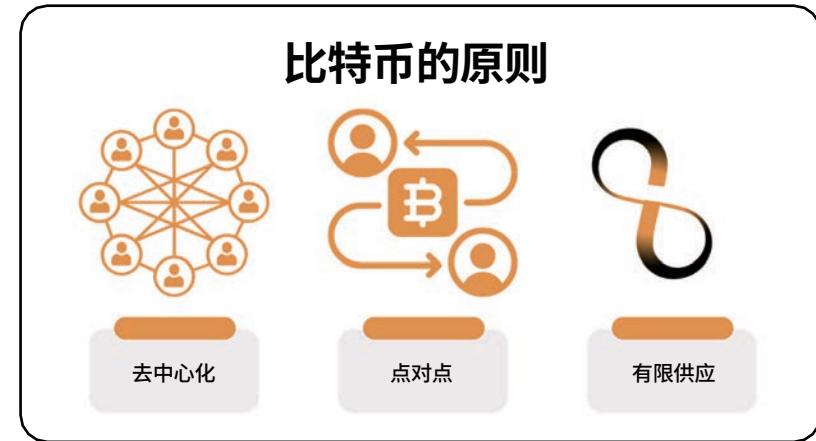
My
First
Bitcoin

HCM®

比特币是完全数字化且无国界的。你在哪里并不重要，因为比特币存在于分布在世界各地的人们的电脑和智能手机上。世界各地的许多用户都在运行比特币软件及其分类账副本。这个软件和所有交易记录消失的概率非常低，因为它有无数个副本。要想关闭它，就必须永远关闭整个互联网，而这几乎是不可能发生的。

最后，比特币是稀缺的，这意味着比特币代币的数量绝对有限。没有人可以伪造比特币，即使是最强大的政府和金融机构。

比特币的原则



6.2.2 比特币的特性

健全货币的演变

正如大家在第2章中所学到的那样，健全货币的生命周期要经过三个阶段才能被人类社会普遍接受：从“价值储存”到“交易媒介”，最后成为“记账单位”。

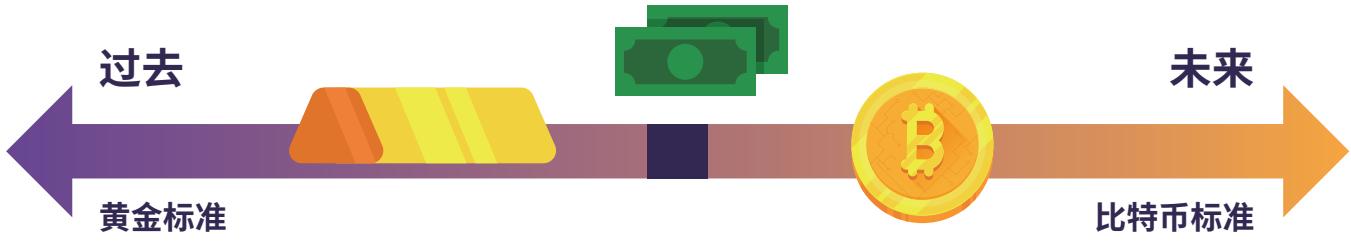
货币的第一阶段的重点是价值储存，即货币作为一种稳定(或升值)的资产，开始随着时间的推移赢得人们的信任。很早就认识到这一点的人们会将财富储存在这种形式的货币中，以保护自己的财富，尤其是在地缘政治和宏观经济充满不确定性的时期。

媒体等一些团体之所以将比特币称为一种“数字黄金”。因为在过去十年中，比特币牢固地确立了自己的价值储存地位。每天都有越来越多的人开始把比特币看作一种对冲通货膨胀的工具，就像黄金在人类历史上一样。

下一阶段是对货币稳定性的信心增强阶段。这时，货币转变为一种交换媒介，为人们日常生活中的交易提供便利。在这一阶段，货币开始被广泛接受，用于交换商品和服务。

比特币正逐步成为一种交易媒介。随着越来越多的商家接受比特币以及比特币协议的发展，比特币交易在日常商业活动中变得更加高效和普遍。萨尔瓦多就是一个例子，该国正式承认比特币为法定货币。因此，每天都有越来越多的普通市民和企业开始使用比特币作为交易媒介。

比特币简介



在最后阶段，货币获得了记账单位的地位，成为商品和服务定价的通用计量单位。在这一阶段，货币成为衡量所有其他价值的标准尺度。

而比特币成为记账单位的过程是一个更加漫长(长期)的过程。目前，世界上只会用法定货币来衡量商品和服务，因此比特币还需要得到更为广泛的采用，并融入各种金融体系。不过，随着企业和个人开始考虑使用比特币并将其作为计价单位，比特币的推广已经奠定了基础。



正如你看到的，比特币在健全货币的进化周期中进展顺利。当比特币完全融入全球金融体系时，它将成为标准记账单位，并重塑整个全球货币体系。



第六章



货币的属性

正如你们在第2章中所学到的，随着时间的推移，人类已经认识到，真正健全的货币必须具备某些特性才能有效。这些特性是：持久性、可分割性、便携性、可接受性、稀缺性和可替代性。

下面让我们看看比特币能否通过测试。

耐用性: 比特币是纯数字货币，因此完全耐用。

可分割性: 作为比较，法定货币美元可以被分割成美分(0.01)。比特币可以分割成所谓的satoshi或sat(0.00000001)。由于比特币的数字特性，在未来如果人类需要，它还可以被分割成更多份。比特币是世界上可分割性最强的货币资产。

便携性: 2020年4月，11亿美元在短短几分钟内就被转走，而且只花了68美分。没有任何其他支付方式能以如此低的成本、如此快的速度，独自转移如此多的资金，这就是比特币成为世界上最容易移动的货币形式的原因。

可接受性: 比特币仍处于成为交易媒介的初期阶段。与法定货币相比，比特币在目前的接受度仍然较低。

稀缺性: 目前只有2100万个比特币，这就意味着比特币不仅稀缺，而且是世界上最稀缺的货币资产。

可互换性: 每个单位的比特币与其他任何单位的比特币都是一样的，可以通过比特币协议进行同类交换和交易，因此比特币是一种可替代货币。

比特币简介

比特币 vs 黄金 vs 美元

货币属性	黄金	法定货币	比特币
耐用性	高	中	高
便携性	中	高	高
可分割性	中	中	高
可替代性	高	高	高
稀缺性	中	低	高
可验证性	中	中	高
历史确立	高	中	低
抗审查性	中	中	高
智能/可编程性	低	中	高

来源：“Bitcoin vs Gold vs US Dollar” Bitcoin Magazine, <https://bitcoinmagazine.com>

比特币是一种智能货币，它可编程，无法被拿走，并具有所有特性，这使其成为储蓄的好帮手，并可以为希望快速交易的商家提供方便。

由于比特币是一个透明的数字账本，因此它在抓欺诈和发现服务中的风险等方面具有超级高的效率。不仅如此，比特币还具有黄金的优点，比如数量有限。比特币也有法定货币的优点，因为你可以把它分割开来，以便携带。此外，它还为我们的数字世界提供了新的功能。

你怎么看？尚未被广泛认可和采用的比特币，能否算是健全的货币呢？



第六章



活动: 课堂讨论——比特币是稳健货币吗?

既然我们已经更为详细地对比特币进行了讨论, 那么就让我们再来看看第二章中的货币对比表, 看看比特币与其他形式的货币的比较。

良好货币的特性	畜牧	香烟	钻石	欧元	比特币
耐用性					
便携性					
统一性					
可接受性					
稀缺性					
可分割性					
总计					

6.2.3 承担个人责任

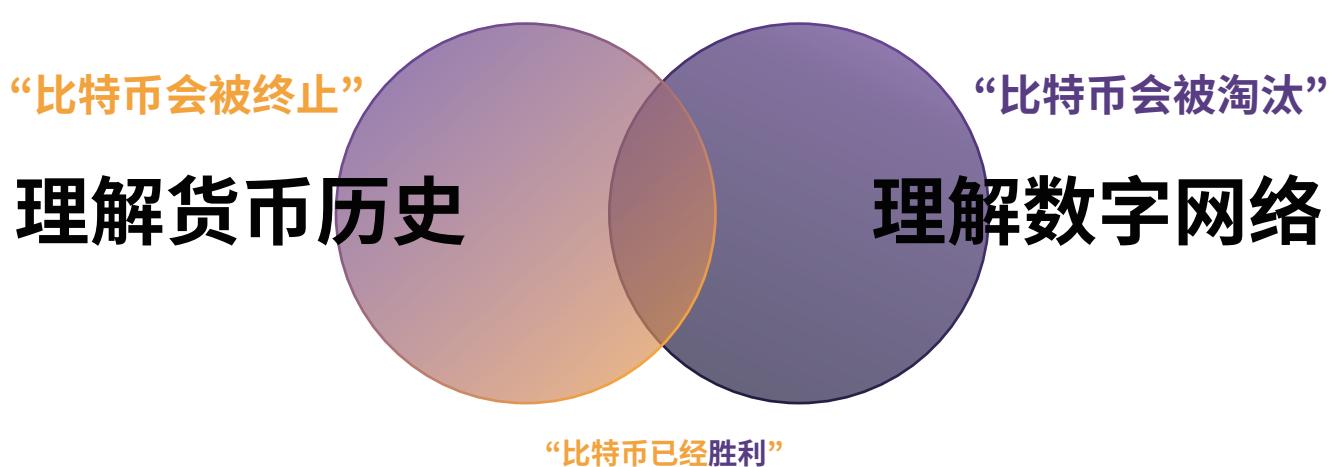
这就是一个没有单点故障的分布式系统。用户持有自己资金的加密密钥, 并在 P2P 网络的帮助下直接相互交易, 以检查是否存在重复消费。

中本聪

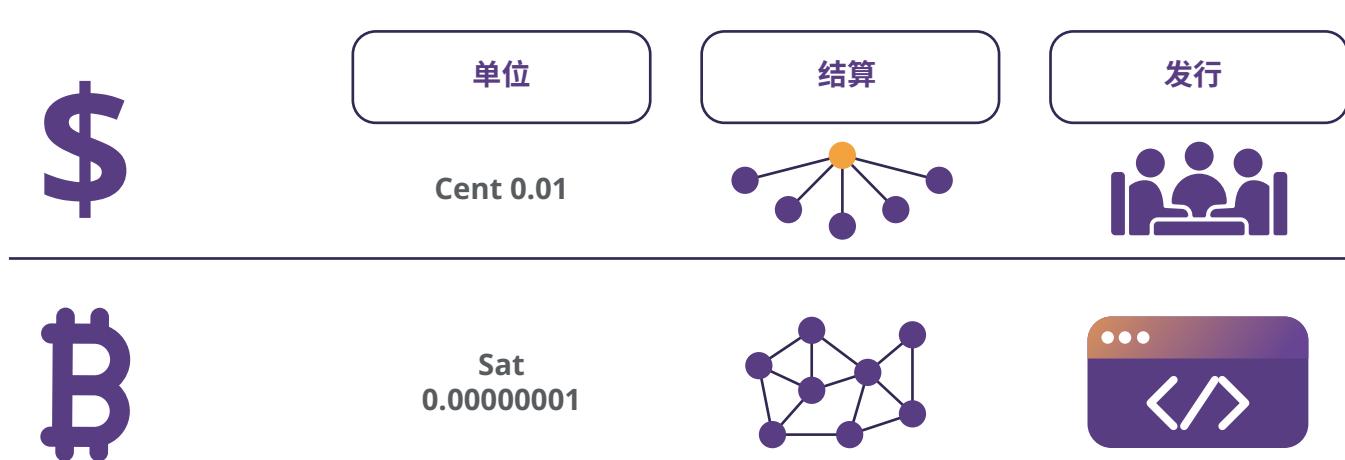
比特币简介

在法币的世界里，人们依赖政府、银行和既定的支付提供商。这些(金融)机构的负责人制定网络规则，而参与者(大多是普通公民)必须遵守这些规则。不管你住在哪里，总有一套标准程序用来指导你做什么、怎么做。这导致随着时间的推移，困难不断循环，对那些在日益严峻的日常生活挑战中苦苦挣扎的家庭而言更是如此。

由于这种制度，人们习惯于将财务责任交到他人手中。例如，大多数人往往都依赖别人来帮助自己，尤其是在出了问题的时候(比如，无法使用银行账户)。



众所周知，比特币的货币体系是非常不同的。比特币以一种特殊的方式运行，其统治者被自主的规则体系所取代。没有独裁者或领导者，也就意味着没有人会对你的行为指手画脚。如果你想从比特币中获得新发现的自由和权力，那么你需要学习比特币是如何运作的，并以适合你个人的方式对这项技术进行整合。





第六章



通过使用比特币，你可以完全控制你的资金，但这种额外的控制也会带来更多的责任。例如，如果你因为丢失了数字钱包的钥匙而无法使用比特币，那么这就意味着你永远失去了你的储蓄。在出现问题时，你没有客服热线可以拨打，也无法向其他人求助。一切问题都需要您自己处理。

幸运的是，这种情况不会发生在那些决定能够完全对自己的生活负责的人身上。使用比特币本身并不复杂，它只是一个新概念。但如果你愿意学习如何使用比特币，并完全承担保护自己财富的责任，那么比特币就会成为一种增强你的能力的工具，因为你可以完全掌控自己的财富，没有人可以将它夺走。

总之，关键在于行动，在于了解比特币的工作原理，并根据自己的独特需求和生活理念来进行实践。接下来，我们将通过设置比特币钱包、发送和接收第一笔交易，以及回顾安全最佳实践来开始使用比特币。

第七章

如何使用比特币

7.0 引言

7.1 获取和兑换比特币

7.1.1 点对点：线下

7.1.2 点对点：线上

7.1.3 集中式交易所

7.2 比特币钱包简介

7.2.1 自托管钱包与托管钱包

7.2.2 不同类型的比特币钱包

7.2.3 开源与闭源

活动: 课堂评估比特币钱包

7.3 设置移动比特币钱包

活动: 设置/恢复比特币钱包

7.4 接收和发送交易

活动: 比特币交易实践

7.5 比特币储蓄

7.6 自己研究 - 不要相信，要验证

如何使用比特币

7.0 引言

为什么会有人相信由一群书呆子创造的比特币，而不是中央银行的钱？
因为这群书呆子给你带来了互联网，而银行给你们带来了大萧条。

安德烈亚斯·M. 安东纳普洛斯

现在，我们已经对比特币及其用途有了更深入的了解，是时候学习该如何实际地使用它了。在本章，我们将引导你逐步完成获取比特币的过程，探索现有的各种类型的钱包，并帮助你设置自己的比特币钱包，甚至练习在网络上发送并跟踪比特币交易。是时候将你的理解转化为行动了！

7.1 获取和兑换比特币

获取比特币的方法有很多。例如，你可以：

- ◆ 用比特币换取工作报酬，用比特币支付他人的产品和服务(详见第8章)。
- ◆ 比特币挖矿(详见第9章)。
- ◆ 将法定货币兑换成比特币，或者在线下将比特币兑换成法定货币。
- ◆ 用法定货币兑换比特币，或者在线上用比特币兑换法定货币。



下面，我们将探讨如何用法定货币兑换比特币，反之亦然。我们既可以通过现场当面交易，也可以通过在线方式进行兑换，因为这两种方式是最常见的。

7.1.1 点对点：线下

参与点对点(P2P)交易以获取和出售比特币，包括直接与他人用法定货币(或任何其他商品或服务)交换比特币，无需银行或其他方参与交易。

双方共同决定兑换金额和兑换率。买方提供现金，卖方转移比特币，交易结束。

虽然在现实世界中直接与对方见面并进行点对点交易更为方便，但你也可以借助互联网，在任何地方进行点对点交易。此外，用比特币兑换法定货币的过程也与之类似。





第七章

**My
First
Bitcoin**

HCM

7.1.2 点对点：线上

进入P2P平台，比特币买家和卖家在网络空间会面，并直接在互联网上进行交易，无需任何中介。

在这样的平台上，你不必把自己的信息或资金托付给任何人。你可以与其他人见面，直接与他们交易。



在大多数P2P平台上，同行都必须托管部分资金，以确保他们履行自己的交易部分。托管意味着将资金放在由平台控制的安全的地方，直到双方都履行承诺。这就像由一个值得信赖的朋友保管着你的东西，直到每个人都信守诺言。

7.1.3 集中式交易所

使用集中式交易所可能是获取和出售比特币最简单的方法，但也涉及重大的利弊权衡。集中式交易所是允许客户直接通过它们买卖比特币的公司。然而，这种便利是有代价的。



集中式交易所及其利弊权衡

值得注意的是，在通过集中式交易所购买比特币时，通常需要提供个人信息并验证身份。这就产生了身份被盗的风险，使你的个人信息面临潜在威胁。此外，集中式交易所为你持有比特币意味着你在从它们那里提取比特币之前，无法控制自己的钱。

更令人担忧的是，中心化交易所可能会挪用用户的资金，或者借出超过其储备的比特币，并最终倒闭——是的，就像银行一样！然而，在比特币世界里，没有中央银行会通过印制更多货币来拯救欺诈的银行，因为你无法印制更多比特币！

中心化

如何使用比特币

7.2 比特币钱包简介

比特币与实物货币不同，它并不实际存在于一个比特币钱包中。比特币存在于比特币网络不断验证和保护的分布式账本中。那么，该如何才能拥有比特币呢？

只有当你拥有私钥时，才能拥有比特币的所有权，因为私钥允许你签署交易并将比特币的所有权从你手中转移给其他人。这就是发送比特币的行为。

鉴于此，让我们一起来看看在使用“**钱包**”一词时所描述的两个概念。



- ✿ 你可以用主私钥(就像密码一样)生成公钥，并将其与他人共享，以接收和发送比特币。
- ✿ 你可以通过手机或桌面界面与比特币网络互动，以获取比特币余额，发送和接收交易，并将它们广播到网络上。下一节将介绍不同类型的钱包，以及它们的优点和利弊。

7.2.1 自托管钱包与托管钱包

在详细介绍不同类型的比特币钱包及其特点之前，先让我们对非托管钱包和托管钱包进行一个重要区分。本表包括两种主要类型的比特币钱包：自托管和托管。你可以了解使用不同钱包类型的好处和风险，以及每种情况下由谁控制比特币。自托管指用户持有私钥，这就意味着他们真正拥有了自己的比特币；而第二种类型是由第三方持有比特币。

钱包类型	谁在控制我的比特币？	优势	风险
自托管钱包	用户	完全控制资金和交易 无需审批流程或账户冻结 不受公司或政府控制 免受任意没收，类似把钱保存在家中	如果恢复短语丢失，无法恢复 客户支持较少 用户需承担全部责任
托管钱包	第三方提供者	访问权限丢失后更易于恢复 提供更便捷的客户支持	资金始终在线，更容易受到黑客攻击和数据泄露 托管方可以控制和冻结账户



第七章

一方面，在自托管钱包(也称非托管钱包)中，你是唯一拥有钱包钥匙的人，可以完全控制钱包的进出。另一方面，在托管模式下，其他人也持有钱包的钥匙，并且可以代表你访问和管理钱包的内容。

- 自托管就像你自己的银行。自托管模式下，交易不受任何政府或公司的控制或授权，但这也意味着你要承担保护比特币安全的全部责任。
- 自托管可确保第三方无法在未经你同意的情况下没收你的比特币。
- 在不确定的情况下，自托管更让人放心，因为你知道自己的比特币是安全的。

根据每个人的需求选择合适的钱包类型至关重要。有时，人们很难区分自己安装的究竟是自托管钱包还是托管钱包。下表显示了两种钱包安装过程中的不同之处。

钱包类型	步骤1： 选择钱包	步骤2： 安装钱包	步骤3： 创建新钱包	步骤4： 保护你的助记词	步骤5： 开始使用你的钱包
自托管钱包	选择自托管 钱包提供商	按照钱包 提供商的说明 进行操作	生成 恢复助 记词 和至少 一个私钥	将 恢复助记词 存放在安全 的地方	开始使用钱包 接收和发送 比特币
托管钱包	选择托管 钱包提供商	按照钱包 提供商的说明 进行操作	在钱包提供 商处创建 一个账户	不适用 (钱包提供商 持有 私钥)	开始使用钱包 接收和发送 比特币



不是你的私钥
就不是你的币

“不是你的钥匙，就不是你的币。”是在比特币持有者中流行的一句话。这句话指如果你不能直接控制与你的比特币钱包相关的私钥，那么你就不能真正拥有比特币。

无论谁访问了你的私人密钥，他都将获得比特币的所有权。这也就是为什么保护私钥不被窥视是最重要的！在本书的后面部分，我们将对几种保护私人密钥的方法进行介绍。

在下文中，我们将只讨论自我托管钱包，即用户拥有自己的密钥并完全控制自己的比特币。

不要担心接下来的内容会变得复杂或者难以理解。这是一个旅程，当你开始更多地使用比特币时，你就会明白更多！

如何使用比特币

7.2.2 不同类型的比特币钱包

根据私钥的创建和存储位置，我们通常会使用不同的名称来描述比特币钱包。如果密钥被存储在智能手机上，我们可以将其称之为“移动钱包”；如果密钥被安全地存储在专用设备上，我们可以称其为“硬件钱包”；如果密钥只存储在纸上，则可以称其为“纸质钱包”。

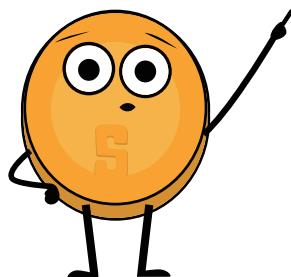
以下表格介绍了我们根据比特币钱包的结构为其所起的名字

钱包类型	描述	优势	劣势	适用用户
在线钱包	通过网络浏览器访问的钱包	可以通过任何有网络连接的设备访问，易于使用	安全性较低，可能会被黑客攻击或泄露	需要频繁访问钱包且没有大量资金存储的人
移动钱包	安装在移动设备上的钱包	方便，可以随时随地访问	如果设备丢失、被盗或被黑客攻击，钱包也会随之丢失	需要随时进行交易且没有大量资金存储的人
桌面钱包	安装在台式计算机上的钱包	比在线钱包更安全，可以离线使用	如果计算机感染了恶意软件，钱包可能会被黑客攻击	想要存储大量 比特币 并且习惯使用台式计算机的人
硬件钱包	用于离线存储 比特币 的物理设备	非常安全，可以离线使用	如果设备丢失或被盗，那么资金可能无法恢复	想要存储大量 比特币 并且愿意为硬件钱包支付额外安全成本的人
纸钱包	比特币钱包的私钥和公钥的物理记录	非常安全，可以离线使用	如果物理记录丢失或被盗，那么资金可能也会丢失	想要存储大量 比特币 并且愿意采取额外的安全措施用以保护资金的人



第七章

由于密钥可以从一个设备转移到另一个设备，因此比特币钱包的“状态”并不确定。例如，如果我在电脑上生成了比特币钱包的密钥，然后将其上传到手机上，那么“桌面钱包”就变成了“移动钱包”。



在存储比特币时，不仅需要考虑谁能控制它，还要考虑许多其他风险。因此，找到一个既安全又方便的存储方案非常重要。

当你分析各种类型钱包的利弊时，会发现根本没有一种理想的钱包能满足所有需求。

在选择比特币钱包时，你需要考虑如下几件事。

-  **安全性:** 确保钱包有强大的安全措施，例如双因素身份验证和安全密码政策。
-  **隐私:** 考虑钱包是否允许你匿名，或者是否需要个人信息才能开设账户。
-  **易用性:** 选择易于使用和浏览的钱包，尤其是当你是比特币新手时。
-  **兼容性:** 确保钱包与你的设备和操作系统兼容。
-  **费用:** 比较不同钱包所收取的费用，以确保你能得到最优惠的服务。
-  **信誉:** 调查钱包及其团队的声誉，以确保其值得信赖。
-  **控制:** 有些钱包能为你提供私钥的更多控制权，这可能是一种安全优势。

考虑一下你是想要一个能让你完全控制的钱包，还是想要一个用户界面更友好，但控制权更少的钱包。

7.2.3 开源与闭源

在选择比特币钱包时，另一个需要注意的重要因素是了解应用程序或软件是否开源。

开放源代码非常重要，因为它允许社区审查代码，并能在团队停止工作的情况下继续开发项目。

如何使用比特币



正如比特币的代码是完全开放的，每个人都可以审查、使用和修改，你用来存储比特币的钱包的代码也应该如此。

活动： 全班讨论并评估bitcoin.org上的比特币钱包

请访问以下网站: <https://bitcoin.org/en/choose-your-wallet>。
利用你对比特币钱包的新知识，根据我们今天讨论的标准选择一个最好的比特币钱包。



7.3 设置移动比特币钱包

现在，既然我们对比特币钱包已经有了更深入的了解，也知道了它们的区别，那么下面我们就来看看在现实中该如何使用一个比特币钱包。在这个例子中，我们将直接在智能手机上创建一个移动钱包。

活动: 设置/恢复比特币钱包

如果学生没有手机，那么老师将向每位学生提供一部手机供其借用。这项活动有以下两种选择。



第七章

My
First
Bitcoin

HCM[®]

课堂练习: 方案1 - 下载新钱包。



如何创建和使用比特币钱包

- 1 在 App Store (iOS) 或 Google Play Store (Android) 中搜索应用程序。
- 2 打开应用程序，输入12或24个字的恢复短语(有时称为种子短语)。请务必将其写下来，并保存在安全的地方！该恢复短语允许你在必要时恢复对资金的完全访问。

请记住，如果你丢失或忘记了这一连串短语，那么你将无法访问你的比特币钱包。

- 3 随后，你必须确认自己确实保存了种子短语。为此，你必须以同样的顺序输入种子短语的单词。
- 4 作为额外的安全措施，有些钱包允许你选择一个安全密码。钱包会自动为你创建私人密钥和第一个比特币地址。

将公共地址视为你的电子邮件地址——你希望与他人共享该地址，因为这样他们就可以向你发送比特币；或者如果是电子邮件地址的话，也可以向你发送电子邮件。

将你的私人地址想象成你的电子邮件密码——你不想与任何人分享这个地址，因为一旦分享，他们就可以访问你的电子邮件。

- 5 使用“接收”地址接收比特币。将比特币转入你的钱包。使用自托管钱包，由于你不可能总是直接用法币购买比特币，因此你可能需要先从交易所购买并进行转账。

如何使用比特币

课堂练习: 选项2 - 恢复钱包 (有时间限制)



下载一个比特币钱包，为每个学生添加一些比特币。

给每个学生发一张印有种子短语的纸，让他们找回钱包。

逐步引导学生

- 1 在首次启动钱包时，你会看到三种创建钱包的方法。点击[导入现有钱包]，你会看到一个介绍界面，然后点击[用恢复短语恢复]。
- 2 按正确的顺序逐一输入你的12/18/24个字符的恢复短语。
- 3 完成后，点击[还原/恢复]。
- 4 成功导入钱包后，你将看到“导入成功”模式。

7.4 接收和发送交易

比特币交易即将现有比特币的所有权转移给一个新的所有者。但在网络中的所有节点，比特币并不会被实际转移，而是更新其本地的公共分类账副本，以反映所有权的变化。

在发送比特币交易时，发送者会用自己的私钥签署一条只有自己才能签署的信息，然后向网络发出信号，比特币的所有权将变更为收件人的地址。

现在，比特币将与一个地址绑定，只有新的拥有者才能从该地址发送比特币，从而获得比特币的所有权。

分类账

账户所有者	余额
山姆	2.50
亚当	3.00
迈克尔	6.00
吉姆	1.50
罗伯特	2.00
埃利安娜	1.75
丹尼尔	5.25

比特币交易
请求消息
吉姆向埃利安娜
发送 0.50 BTC
吉姆 ▶ 埃利安娜
0.50 BTC

账户所有者	余额
山姆	2.50
亚当	3.00
迈克尔	6.00
吉姆	1.00
罗伯特	2.00
埃利安娜	2.25
丹尼尔	5.25

新的比特币交易由世界各地的钱包发起，但没有中央支付处理器。与之相反的是，世界各地的矿工竞相将交易记录到分类账中。

假设吉姆欠埃利安娜 0.5 BTC，并准备还给她，而两人都有数字钱包。





第七章

- 1 埃利安娜向吉姆分享了自己的地址。
- 2 吉姆使用钱包软件创建交易，其中包括埃利安娜的地址、转账金额(0.5 BTC)和矿工费用。
- 3 签署交易后，交易被广播到网络，由节点进行验证。节点会检查交易的有效性，以确保吉姆有足够的资金。如果没有，节点则会立即拒绝交易。
- 4 一旦交易得到验证，矿工就会将其添加到区块链中，而资金就会被转移到埃利安娜的地址。
- 5 随后，埃利安娜就可以使用自己的私人密钥访问钱包中转来的资金。

值得注意的是，交易一旦完成，就不能撤销。



接收比特币交易

要接收比特币，就需要向发送者提供你的比特币钱包地址。那是由字母和数字组成的唯一字符串，用于在比特币网络中识别你的钱包。你可以登录比特币钱包，在“接收”或“存入”比特币选项中找到你的钱包地址。

然后，你可以通过以下几种方式与发送者共享你的比特币地址。

- 1 复制并粘贴地址：你可以选中地址并按键盘上的“复制”键来复制地址，然后将其粘贴到给发送者的电子邮件或信息中。
- 2 共享你的比特币钱包链接：有些比特币钱包允许你创建一个钱包链接，与发送者共享。然后，他们就可以点击链接访问你的钱包并发送比特币。
- 3 分享二维码：如果发送者拥有装有比特币钱包应用程序的智能手机，那么他们就可以扫描二维码并获取你的比特币地址。

如何使用比特币

发送者一旦有了你的比特币地址，就可以通过输入你的地址和他们想发送给你的比特币金额来给你发送比特币，并启动交易。然后，比特币将被发送到你的钱包。一旦交易在比特币网络上得到确认，你就可以看到比特币了。这通常另需要几分钟时间。

接下来，让我们来看看发送比特币交易。

发送比特币交易

要发送比特币，你需要几样东西：比特币钱包、接收人的比特币地址和你要发送的数额。

- 1 打开比特币钱包。系统会向你的手机号码发送短信验证码，而你需要在对话框中输入验证码。如果你已启用 Google 2FA，则需要在Google Authenticator 应用程序中输入六位数代码。
- 2 使用“发送”或“取出”功能并复制收件人地址。
- 3 在“接收人”栏粘贴接收人的比特币地址。
- 4 在“金额”栏中输入你要发送的比特币金额。
- 5 仔细核对收件人的地址和发送金额。
- 6 在点击“确认并发送”之前，我们建议你再仔细检查一次交易细节，以确保你向正确的钱包地址发送了正确数量的比特币。
- 7 确认交易并等待网络确认交易。

现在你知道该如何评估、选择和设置一个自我保管的比特币钱包了吧。在比特币网络上，从一个钱包向另一个钱包发送比特币被称为发送“链上”交易，因为交易发生在比特币主网的区块链上。链上交易是使用比特币进行交易的最安全方式。不过，与我们将在第8章讨论的其他方式相比，链上交易的成本更高、速度更慢。

活动: 比特币交易实践

目的: 了解点对点比特币交易的基本概念和机制。

在开始之前，让我们先来简单介绍一下比特币交易中的主要参与者。

- 发送方和接收方是希望进行交易的双方。
- 节点验证交易并存储区块链的完整副本。
*轻节点可以让人们在使用较少存储空间和计算资源的情况下对交易进行验证。
- 矿工负责向区块链添加新的交易。



第七章

了解自己的角色。你已被分配了以下之一的角色：发送者、接收者、节点或矿工。

-  发送者将负责创建和广播交易。
-  收款人将负责接收和核实交易。
-  节点将负责验证交易，检查交易是否有效。
-  矿工将负责把交易添加到区块链中。

节点和接收方都必须验证交易

作为发件人: 创建交易。

如果要创建交易，请按照以下步骤进行操作：写一张交易单据，写上要发送的硬币数量和接收人的姓名或姓名首字母；用你的姓名或姓名首字母在纸条上签名，模拟私钥；将交易单据和相应数量的硬币交给接收方。

作为接收方: 你负责核实交易。

-  检查交易单据，以确保硬币数量和收款人姓名或姓名缩写正确无误。
-  清点收到的硬币，并与纸条上写的硬币数量进行比较。
-  如果硬币匹配，请在框里打勾；如果硬币不匹配或你有疑问，请拒绝交易。

比特币已发送	发送人	发送人签名	接收人	日期 & 时间	接收人确认

作为节点: 由你负责验证和确认交易，检查交易是否有效。

-  验证发件人和收件人地址是否有效。
-  检查发送方是否有足够的资金完成交易，以及交易是否重复花费任何硬币。

比特币已发送	发送人	发送人签名	接收人	日期 & 时间	接收人确认

如何使用比特币

4 作为矿工: 由你负责将交易添加到区块链中。

请按照以下步骤操作:

- ✿ 检查已由接收方批准并由节点验证的交易。
- ✿ 掷骰子并与其他矿工比较数字，其中数字较小的矿工将把交易添加到区块链中。
- ✿ 你付出的时间、精力和努力将为你赢得一分。活动结束时，积分最多的矿工获胜。

**交易一旦添加到区块链中，就无法更改或撤销。

5 记录硬币余额: 在整个活动中，通过清点数字钱包中的硬币来记录硬币余额。

比特币已发送	发送人	发送人签名	接收人	日期 & 时间	接收人确认

6 与全班讨论所学概念。

7.5 比特币储蓄

如果操作得当，那么比特币既是一种可以保护你的钱财不受通货膨胀影响的方法，也是一种保护你的钱财不受他人控制的方法。比特币储蓄是一种长期储存、积累和创造财富的工具。正如你现在所理解的，选择哪种储蓄方式是你所能做出的最重要的决定之一。明智的选择可以让你为自己和家人创造更美好的未来。



放心: 在妥善保管的情况下，比特币是唯一一种无人能夺走的财产形式。





第七章



7.6 自己研究——不要相信，去验证

无论你在比特币的世界里做什么，请记住：“不要相信，要验证。”比特币没有领导者。你永远不应该盲从别人的说法。相反，你应该质疑别人告诉你的东西，并亲自验证。只要遵循这个原则，你就能保护自己的比特币，使其不受损失。这一点适用于“下一个比特币”等说法，就像适用于“投资机会”或“快速轻松获利”的承诺一样。

总之，第7章让你掌握了在日常生活中使用比特币的重要技能。你已经学会了该如何以不同的方式获取和兑换比特币，以及该如何使用各种钱包以保护比特币的安全。

通过设置你的移动比特币钱包并与他人进行交易，你现在已经拥有了在日常中使用比特币的实践经验。通过了解到比特币是一种省钱的方式这一概念，并遵循“自己研究DYOR(Do Your Own Research)——不要相信，去验证”的理念，你现在就可以掌控自己的钱了。

在接下来的章节中，我们将探讨闪电网络。我们将了解这项创新技术是如何改变世界各地的人们获取和使用货币的。从日常交易到更先进的应用，你将了解闪电网络是如何通过为个人、社区和企业提供金融服务来增强他们的能力的。

第八章

闪电网络： 将比特币融入日常生活

8.0 引言

活动: 观看《比特币闪电网络解析：它是如何运作的》

8.1 闪电网络

8.2 不同类型的闪电钱包

8.2.1 自托管钱包与托管钱包

8.2.2 开源与闭源

8.3 创建一个比特币闪电钱包

8.4 闪电交易的发送和接收

活动: 闪电钱包接力赛

8.5 用比特币购买咖啡和日用品

8.5.1 线上：支付插件 - 电子商务

8.5.2 线下：寻找本地商家

8.5.3 过渡工具：礼品卡与支付卡

8.5.4 循环经济与比特币作为交易媒介

闪电网络： 将比特币融入日常生活

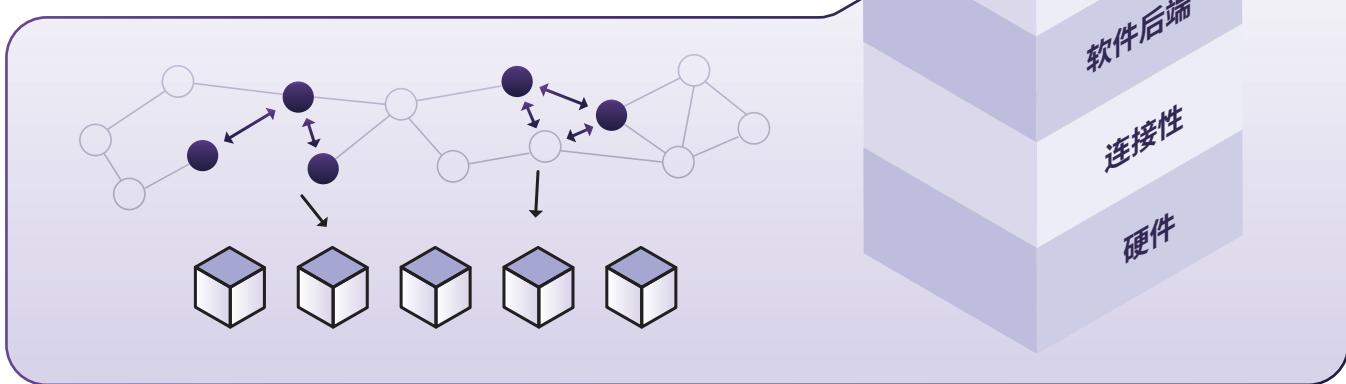
8.0 引言

我们正在为比特币打造Visa网络。但我认为比特币的强大之处在于其与Visa不同，任何人都可以在它的基础上进行开发。

伊丽莎白·斯塔克

技术就像堆栈一样通常是分层发展和扩展的。想想你最喜欢的网站、电子邮件或社交媒体：它们建立在互联网协议之上，而互联网协议又建立在计算机之上，计算机又建立在电力之上，等等。这些技术最初的设计都非常简单，并会随着时间的推移而不断改进。

比特币也不例外。正如安德烈亚斯·安东纳普洛斯(Andreas Antonopoulos)的名言：“比特币是货币互联网。”比特币是健全数字货币的基础层，它为新技术的发展提供了坚实的基础。



其中一层被称为“闪电网络”。闪电网络就像比特币的超高速高速公路，可以帮助人们以非常低的费用快速收发比特币。闪电网络允许用户在普通比特币网络之上进行即时小额交易。这使得买杯咖啡或付钱给朋友变得简单快捷！

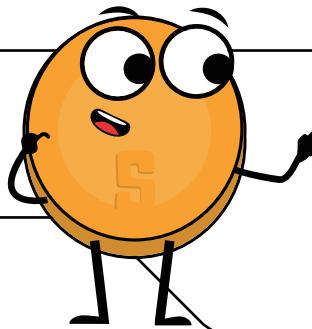
记住：sat就像比特币最小的硬币。就像一美元可以分成几美分一样，一个比特币也可以分成更小的单位，即“sat”。一个比特币等于一亿个sat，因此sat是比特币系统中最小的价值单位。在本章中，我们称通过闪电网络发送比特币为“发送sats”。sat只是一个比特币的比较小的一部分。

聪	比特币
1	0.00000001
10	0.00000010
100	0.00000100
1,000	0.00001000
10,000	0.00010000
100,000	0.01000000
1,000,000	0.10000000
10,000,000	0.10000000
100,000,000	1.00000000



第八章

活动: 观看这个关于闪电网络的视频



8.1 闪电网络

正如我们所看到的，闪电网络是一个可促进比特币快速且低成本交易的支付系统。闪电网络的运作方式是建立一个共享钱包，双方都持有一些比特币。他们可以在彼此间进行大量交易，而无需在主分类账上记录每一笔交易。交易完成后，最终余额会被记录在分类账上。



闪电网络是一种支付系统，允许用户快速且低成本地使用比特币进行支付和接收款项。闪电网络的运作方式是通过建立一个共享钱包，让双方将比特币存入其中，然后在彼此之间进行无限次交易，而无需触及主区块链。当交易完成时，最终的余额才会被记录到主区块链上。

想象一下在咖啡馆的一天。由于预计要在这里度过一整天，你预付了一笔钱，而不是每次点餐时都付钱。当一天结束，你准备离开时，你和店主会查看账单并结清最终账单。如果你支付的费用高于实际消费，那么你就会收到一些退款。

现在，设想一下成千上万的人同时做同样的事情，而他们的账单可以和其他人链接，这就是闪电网络！

通过使用闪电网络，你可以向网络上的任何人付款，而不仅是与你拥有链接的人。即使你与收款人之间没有开放的通道，你的付款也可以在网络中到达目的地。

让我们来看看链上交易(我们在第7章中讨论过的类型)和链外交易(闪电网络)之间的区别。

链上交易

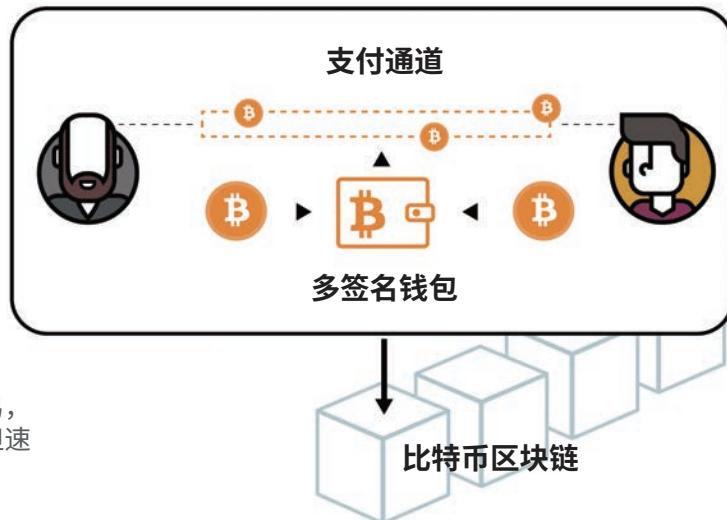
即直接在比特币区块链上进行的交易。确认链上交易需要大约10分钟，其费用取决于交易的字节大小。链上交易更安全，但速度较慢。



闪电网络： 将比特币融入日常生活

链外交易(闪电网络)

链上交易发生在比特币区块链之上的独立网络上。它们的结算速度更快、费用更低。它们通常被用于法规和法律支持采用它们的地方，交易速度和成本等功能在那些地方更加重要。与链上交易相比，链上交易的安全性较低。



总体而言，闪电网络可以实现近乎即时的交易，且费用超低；而比特币交易虽然非常安全，但速度较慢，且费用较高。

支付网络	比特币网络	闪电网络
定义	一个去中心化的数字网络，使用密码学来保障金融交易的安全性	基于比特币区块链的第二层支付协议，可实现更为快速、廉价的交易
优点	去中心化且安全，无退款或欺诈风险；可以匿名使用，具有全球接受度	交易速度更快、成本更低；提高了可扩展性；链外交易不会堵塞区块链
缺点	交易速度较慢，某些交易类型费用较高，且对初学者来说较复杂	需要信任通道运营者；仍在实验阶段，尚未被广泛采用；开通和关闭通道需要链上交易



第八章



8.2 不同类型的闪电钱包

闪电钱包与比特币钱包虽然有所不同，但功能相同：接收和发送比特币。其不同之处在于，闪电钱包允许你在闪电网络上发送比特币，而闪电网络本身就是比特币网络的第二层。

正如我们在上一章中看到的比特币钱包一样，闪电钱包也各有其特点，因此在选择前需要考虑清楚。

8.2.1 自托管钱包与托管钱包

可以将闪电钱包细分为非常具体的类别。但为了简单起见，我们可以主要将它们分为两种：自托管钱包和托管钱包。

就像比特币钱包一样，自我托管的闪电钱包即由你自己控制钱包密钥的钱包，托管闪电钱包则是由其他人控制密钥的钱包。

在使用托管钱包时，你只能访问钱包，需要依赖他人的许可才能使用您的资金。为了方便起见，你放弃了对资金的所有权。

对小额资金来说，这种方式是可以接受的。不过，建议你还是在了解该技术后再使用自托管钱包。

在下文中，我们只讨论自托管的闪电钱包。

8.2.2 开源与闭源

就像我们在上一章看到的比特币钱包一样，闪电钱包既可以是开源的，也可以是闭源的。一定要使用开源钱包，因为它们是完全开放的，以供社区审查和审核。

开源应用程序还意味着任何人都可以为软件的改进做出贡献，从而使其成为对用户来说更好的选择。

8.3 创建一个比特币闪电钱包

创建一个自托管的比特币闪电钱包和创建一个自托管的比特币链上钱包的步骤相同。

闪电网络： 将比特币融入日常生活

课堂练习 - 选项1: 下载一个新的自我托管闪电钱包

如何创建和使用比特币闪电钱包。

-  1 在App Store (iOS)或Google Play Store (Android)搜索应用程序。
-  2 打开应用程序，输入12或24个字的恢复短语(有时称为种子短语)。请务必将其写下来并保存在安全的地方！这个恢复短语允许你在必要时恢复对资金的完全访问。
-  3 然后，你必须确认自己确实保存了你的恢复短语（或种子短语）。为此，你必须以同样的顺序输入你的种子短语的单词。
-  4 作为额外的安全措施，有些钱包允许你选择一个安全密码。钱包会自动为你创建私人密钥和第一个比特币地址。
-  5 生成一个闪电收款单、地址或二维码来接收比特币。将比特币转入你的钱包。当你使用自托管钱包时，不可能总是直接用法币购买比特币，因此你可能需要先从交易所购买比特币并转账。

您的种子短语

您的种子短语可以用于生成和恢复您的账户。

1 Issue	2 Flame	3 Sample	4 Lyrics	5 Find
6 Vault	7 Scissors	8 Banner	9 Cute	10 Damage
11 Civil	12 Goat			

请将这12个单词写在纸上，请注意他们的顺序很重要。这个种子短语将允许您恢复自己的账户。

*注意: 如果你使用的是托管钱包，则无需遵循第8.3节中的某些步骤。使用托管钱包是有风险的，因为你无法控制你的私钥，所以这就意味着你无法控制自己存放在钱包里的钱。

现在我们已经设置好了比特币闪电钱包，接下来让我们来看看闪电交易的接收和发送，以及它们与我们在第7章中发送的链上交易有什么不同。



第八章

 My
First
Bitcoin

 HCM

8.4 闪电交易的发送和接收

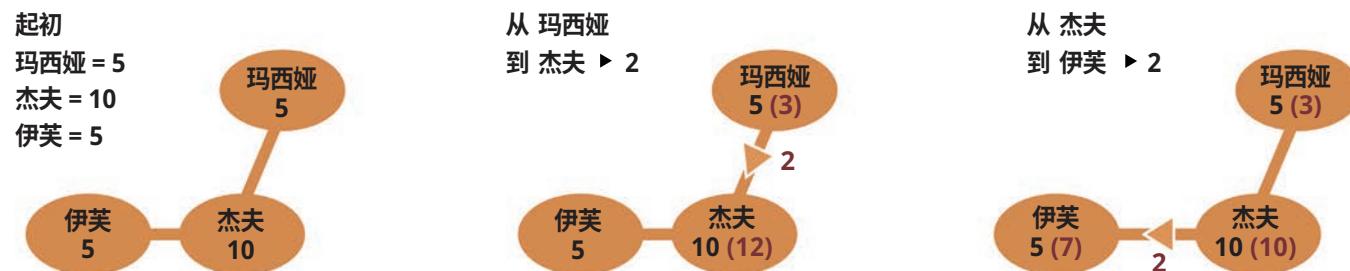
有了闪电钱包，使用比特币就变得快速、便宜、私密，两个人之间的交易因而变得简单。你可以快速收发比特币，用于购买咖啡或购物等日常事务。

让我们来看几个闪电网络的实例。

例1：

如图，玛西娅有5个单位的某种货币，伊芙也有5个单位。玛西娅想把其中2个单位发送给伊芙，于是她发送了2个单位给杰夫。然后杰夫把这2个单位转给伊芙，于是伊芙现在有7个单位，玛西娅现在有3个单位。交易就这样完成了！

以上内容的关键在于，玛西娅和伊芙无需通过银行或其他中介机构来实现交易。



在这种情况下，玛西娅和伊芙并不直接相信对方，而是由杰夫充当中间人或“可信的第三方”。杰夫从玛西娅那里收到了2个单位，然后转交给伊芙，从而完成交易。通过以杰夫作为中间人，玛西娅和伊芙无需银行或其他中央机构即可完成交易，从而使交易变得更快、更便宜、更安全。杰夫是点对点交易过程中的关键因素。

作为闪电网络交易中的节点操作员，杰夫可以从多个方面获益。

1 交易费用

杰夫可以从通过他的节点的每笔交易赚取少量费用，这是对他为维护和运行节点所付出的时间和精力的补偿。

2 网络参与度

杰夫通过运行一个闪电节点的方式参与网络，帮助提高网络的去中心化、安全性和稳定性。这可以提高杰夫作为一个可靠节点运营商的声誉和可信度，使他在未来交易中成为更具吸引力的中介。

闪电网络： 将比特币融入日常生活

3 网络增长

随着闪电网络的发展和使用它的越来越多，通过杰夫节点的交易数量可能会有所增加，从而增加交易费收入。

4 提高网络安全性

作为中间人，杰夫在玛西娅和伊芙之间增加了一层保护，这有助于提高网络的安全性。这可以增强用户对网络的信心，使其对新用户更具吸引力，并有助于推动其增长。总之，成为闪电网络的节点运营商可以为杰夫提供稳定的收入来源，并有机会为网络的增长和发展做出贡献。

总之，链上交易速度较慢，但安全性较高；链外(闪电网络)交易速度较快，但安全性较低。

你应该根据自己的需求，在安全性和速度之间权衡利弊。

例2：

米娜对麦当劳情有独钟，每天都去那里吃早餐、午餐和晚餐！

面对这么多不同的支付方式，米娜不知道哪一种才是最好的选择。幸运的是，她对比特币和闪电网络有一些了解。在进行了比较之后，米娜毫不犹豫地选择了闪电支付作为支付方式。

闪电网络 vs 传统银行系统

优势	闪电网络	传统银行系统	优势	闪电网络	传统银行系统
速度	快	慢	可扩展性	高	低
透明性	透明	不透明	隐私性	高	中等
安全性	安全	不安全	互操作性	高	低
交易费用	低	高	法律合规性	中等	高
金融包容性	高	有限	成本效益	高	中等

Visa公司



平均每秒处理
1,700 笔交易。

每秒处理能力为
65,000 笔交易。

比特币链上



每秒处理能力为
7 笔交易。

比特币闪电网络



每秒处理
数百万笔交易。



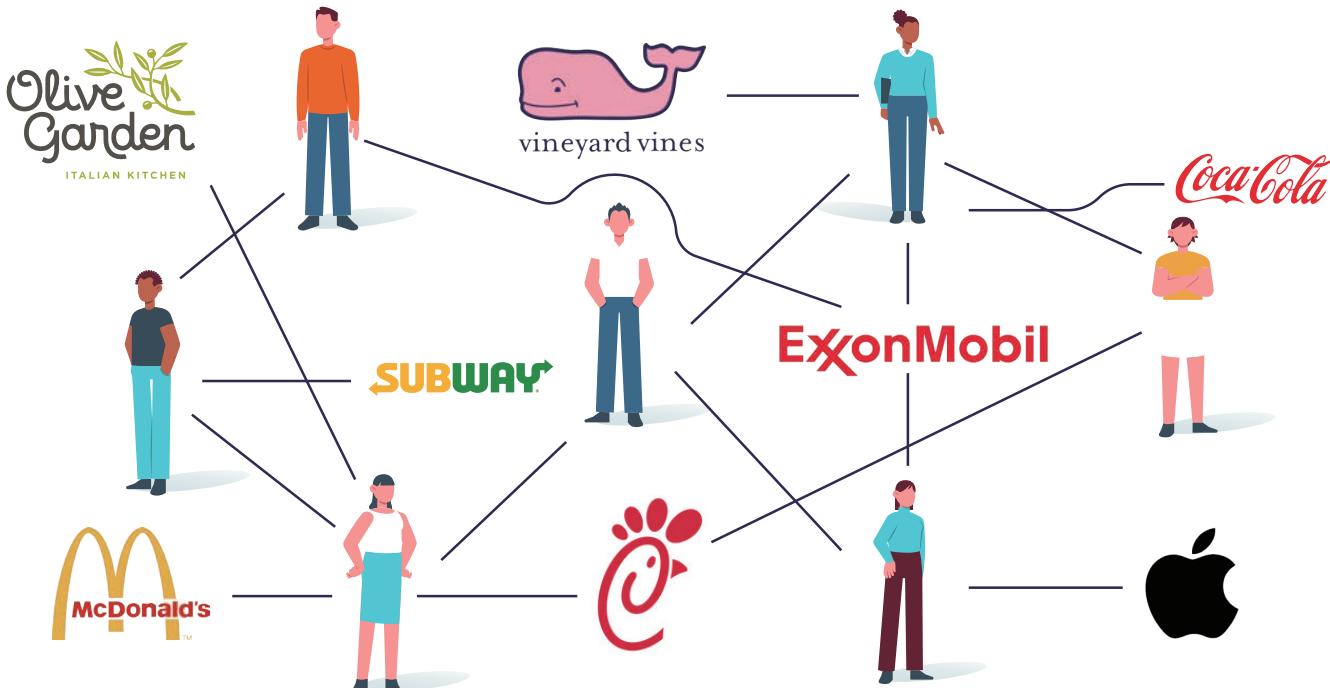
第八章

My
First
Bitcoin

HCM®

米娜也是快速、安全和低成本交易的拥趸者，因此她决定在麦当劳购物时使用闪电支付。有了闪电支付，她就可以更尽情地享受美食了，因为她知道自己的付款即时、安全又实惠。此外，由于闪电网络可以提供普惠金融服务，所以即使米娜身在萨尔瓦多的偏远地区，也可以支付餐费。

要开始使用闪电支付，米娜首先就要在手机上下载一个“闪电钱包”。然后，米娜从普通比特币钱包向新的闪电钱包发送一些比特币，为闪电钱包充值。这个过程被称为“为钱包充值”或“为支付渠道充值”。米娜可以用任意数量的比特币为钱包充值，但需要注意的是，她锁定在闪电钱包中的比特币的数量不能用于链上交易。



一旦米娜的闪电钱包有了资金，她就可以用这些资金向麦当劳付款。

由于麦当劳有一个闪电节点，所以米娜可以通过从闪电钱包中发送一些比特币到麦当劳提供的特定地址，与麦当劳建立支付通道。这就把她的比特币从比特币区块链转移到了闪电网络的链外交易之中。

随着支付通道的开通，现在米娜可以直接在麦当劳购物，而不必开通新的通道，也不必每次都支付高昂的费用。只要米娜和麦当劳都想使用，该通道就会一直开放。例如，如果米娜用0.0005个比特币买了一个汉堡包，那么这个通道就会记录米娜现在有0.9995个比特币。如果她第二天用0.0003个比特币买了一杯奶昔，这个频道就会记录米娜现在有0.9992个比特币。

闪电网络： 将比特币融入日常生活

当米娜决定用她的比特币余额做其他事情时，她就会通过向比特币区块链广播关闭交易来关闭通道。具体做法是在她的闪电钱包中启动关闭交易，交易中包含双方同意的通道最终余额。然后，该交易就会被广播到比特币区块链，并由矿工确认。交易确认后，通道关闭，通道中剩余的比特币将返还给米娜和麦当劳。

值得注意的是，关闭通道后需要一段时间才能在区块链上确认。资金在等待期间仍被锁定在通道中，因此不能用于链上交易。一旦确认关闭交易，米娜就会收到通知。

现在，既然我们已经设置了闪电钱包，也阅读了该如何使用闪电网络发送交易的相关信息，接下来就让我们来玩一个游戏——通过闪电网络向班上其他同学发送sats(比特币的最小单位)。



这是一张世界地图。通过使用闪电网络，你可以向网络上任何拥有比特币闪电钱包的用户发送sats。几秒钟内付款即可到达，而且只需花费几美分。

自己查看一下：





第八章

 My
First
Bitcoin

 HCM[®]

活动: 课堂练习 - 闪电钱包接力赛

1

首先, 你需要在手机或电脑上下载一个闪电钱包。

2

按照本章第8.3节中的说明在设备上安装钱包。

3

钱包安装好后, 打开钱包并按照提示进行设置。这可能需要你创建一个新钱包或恢复现有钱包, 并使用密码或其他形式的身份验证对其进行保护。

4

生成闪电收款单、地址或二维码用以接收比特币。

5

当你设置好钱包并准备好接收比特币时, 老师就会直接将比特币发送到你的钱包中, 从而为你和你的小组提供一定数量的比特币。



A

你们小组的目标是利用闪电网络将比特币从一个人的钱包传递到另一个人的钱包, 直到传递给小组的最后一个人。

B

当你要向他人发送比特币时, 请打开你的钱包并按照说明进行支付。你需要提供收件人的闪电收款单或扫描二维码, 并输入你要支付的比特币的金额。

C

如果你所在的小组是第一个成功将比特币发送给最后一个人的小组, 那么你们就赢了! (你们就可以保留比特币)。

讨论你们小组在活动中所遇到的困难。发送交易是否简单、快捷、便宜? 你认为闪电网络容易使用和理解吗?

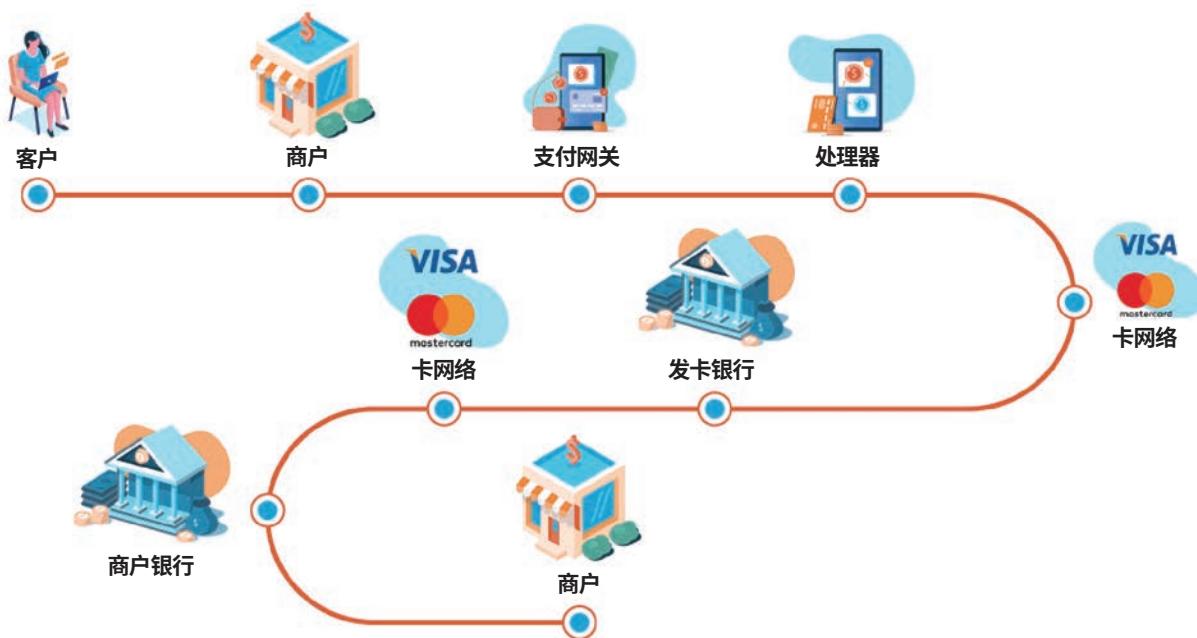
闪电网络： 将比特币融入日常生活

8.5 用比特币购买咖啡和日用品

你是否想过平时可以用比特币购买咖啡或囤积杂货？其实这完全是可行的。有很多网上的商店或实体店都可以用比特币支付。我们将探讨其中一些选择和工具，它们可以帮你找到当地可以用比特币消费的商店。

尽管对于付款人来说，使用信用卡或应用程序进行付款更容易理解；但实际上，处理付款的过程非常复杂，涉及许多不同的方面。

支付处理流程



当你买东西时，往往会牵涉多方，而每一方都会收取一定的费用。对于店主来说，这笔超过商品价格3%的费用对他们来说是一笔不小的数目。

然而，这还不算货币兑换费！



第八章



信用卡处理费用



有了比特币和闪电网络，企业就可以通过一个开放、安全、互联网本地化、无国界和抗审查的货币系统接收来自世界各地的即时付款。

接下来，我们将介绍让几种商家可以轻松接受用比特币支付的方法。

8.5.1 线上：支付插件 - 电子商务

BTCPay Server是一款开源支付处理器，商家只需掌握少量的技术知识，即可接受比特币支付。这款处理器不收取任何佣金，完全免费。

在线企业只需在其网站上添加BTCPay插件，即可无缝集成BTCPayServer。

The screenshot shows the BTCPay Server dashboard. At the top, a large green banner reads "成为你自己的支付处理器。". Below it, a QR code is displayed with the text "Open in wallet". To the left, a table lists several invoices with columns for Date, Orderid, Invoiceid, Status, and Amount. One invoice is marked as paid. On the right, there's a summary section showing "Awaiting payment..." and "Pay with Bitcoin (BTC) 0.0000010 BTC".

闪电网络： 将比特币融入日常生活

由于 BTCPay Server 是一个开源项目，而不是一家公司，因此你只需要对该项目和计算机编程有更多了解，就可以为该项目做出贡献。

查找BTCPayServer
<https://btcpayserver.org/>
了解更多关于如何在个人或在线业务中使用该支付系统的信息。



8.5.2 线下： 寻找本地商家

实体商店也可以使用BTCPay Server 接受付款, 或者干脆下载一个比特币钱包, 直接用手机接受比特币付款。



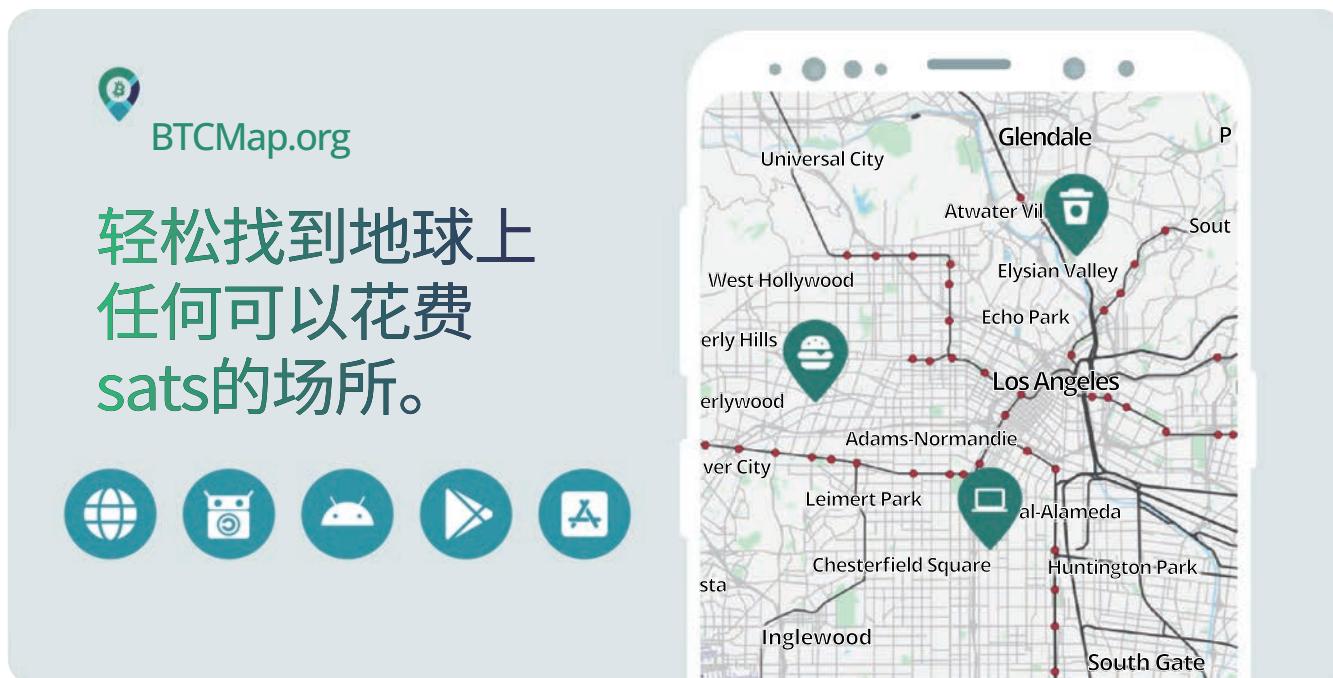


第八章



要想找到你所在地区能够接受比特币的商家，请访问BTCMap.org并搜索你所在的地区。

这是一个开源地图，接受比特币的商家可以在上面列出他们的业务。对于希望使用比特币的人们来说，BTCPay Server无疑是一个强大的工具。



8.5.3 过渡工具：礼品卡与支付卡

如果你想从还不接受比特币的商家那里购买产品或服务，那么你可以使用一种中介工具：礼品卡。

有些商家专注于通过买卖礼品卡来换取比特币。也就是说，你可以用比特币换取你想去的商店的礼品卡，然后直接去相应商店消费。

机票、酒店、游戏、SIM卡……你几乎可以用比特币和礼品卡购买任何东西！

8.5.4 循循环经济与比特币作为交易媒介

循环经济的概念来自通过重复使用和回收尽可能多的产品和副产品，最大限度地减少经济中的浪费。

根据这一概念进行延伸，比特币循环经济是一种用比特币进行交易的经济，比特币形式的货币在经济中得到保持和增长，从而使经济中的个人和企业受益。



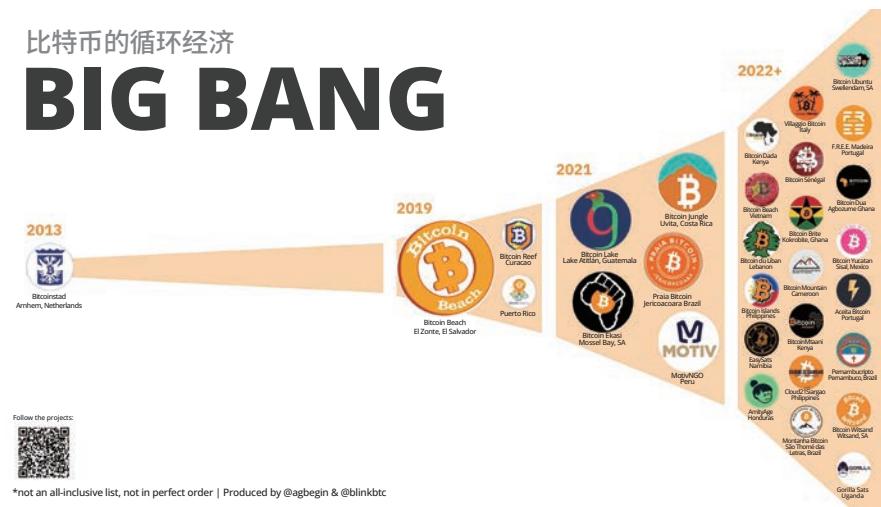
闪电网络： 将比特币融入日常生活

由于比特币交易近乎即时且费用低廉，所以闪电网络使比特币循环经济在世界各地蓬勃发展。



第一个比特币循环经济体位于荷兰阿纳姆。这个经济体是在闪电网络出现之前创建的，但那时链上费用非常低！

比特币的循环经济 **BIG BANG**



第二个比特币循环经济体位于萨尔瓦多埃尔宗特的比特币海滩。通过利用闪电网络的力量，它为大部分没有银行账户的社区提供了直接使用智能手机进行即时数字支付的服务！

如今，在比特币、闪电网络和教育资源的推动下，
世界各地数以百计的循环经济体正在创建中。





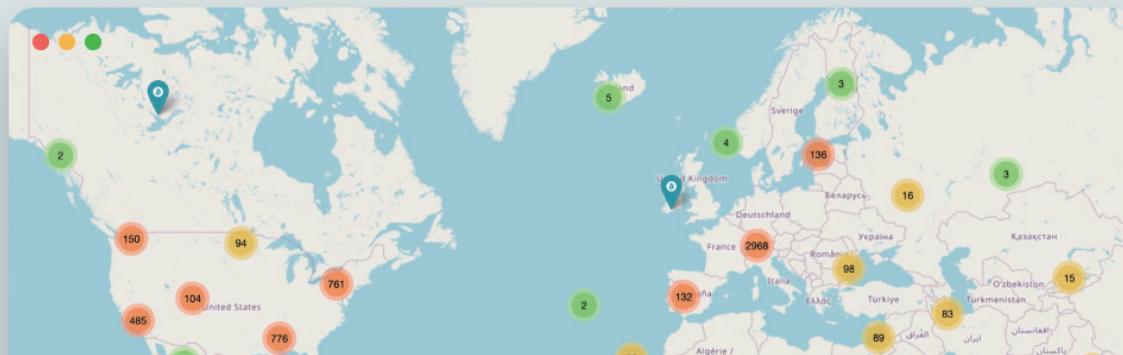
第八章



在BTCMap.org上，你还可以寻找到比特币社区，并在那里认识其他比特币用户，找到可以接受比特币的企业。我们的一些老师和学生已经在BTCmap.org上添加了企业和循环经济，只要准备好了，你也可以加入哦！



轻松找到地球上任何
可以花费sats的场所。



资源: btcmap.org/communities

当第8章结束时，你已经通过闪电网络深入地了解了该如何在日常生活中使用比特币。闪电网络使交易更快捷、更方便，同时预示着比特币会如何不断地变化和发展。

在第9章，我们将从技术层面研究比特币——从密码学到节点、矿工等，准备好近距离了解比特币的真正运作方式吧！

第九章

从技术层面 介绍比特币

9.0 引言

活动: 观看《比特币的技术原理详解》

9.1 公钥与私钥：通过加密技术实现安全

9.1.1 公钥/私钥的加密原理

9.1.2 哈希的解释

活动: 生成 SHA-256 哈希值

9.2 UTXO 模型

9.3 比特币节点和矿工

9.3.1 什么是比特币节点，我又该如何设置？

活动: 观看关于比特币节点的视频

9.3.2 什么是比特币矿工，挖矿是如何进行的？

9.4 什么是内存池？

活动: 内存池

9.5 比特币交易如何从开始到完成

从技术层面介绍比特币

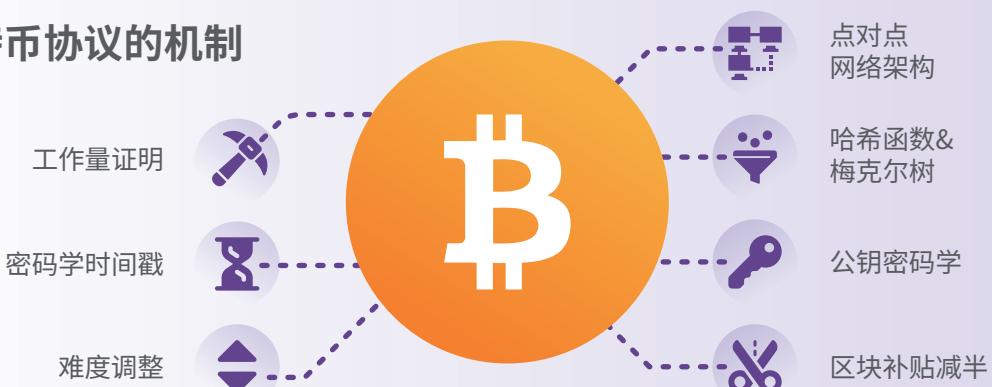
9.0 引言

比特币并非“不受监管”，而是只受算法监管，不被政府官僚机构监管。并且比特币并不腐败。

安德烈亚斯·M. 安东纳普洛斯

在本章中，我们将就支持比特币网络以完全去中心化方式运行的技术进行深入探讨。我们会以简单易懂的方式解释比特币交易的流程，包括当你发送一笔比特币交易时会发生什么、这些交易是如何处理的，以及矿工和节点在比特币网络中所扮演的角色。本章将涉及一些具有挑战性和技术性的概念。需要记住的一点是：许多人并不了解互联网的运作原理，但他们仍然能够每天都使用互联网来发送电子邮件、与社交媒体上的朋友联系，甚至支付账单。同样，即使并非每个人都选择深入了解比特币的技术原理，大家仍然可以选择将其作为货币使用。虽然我们鼓励你持续从技术层面学习比特币，但本章将重点关注比特币较为基本的关键概念，以确保内容清晰易懂。

比特币协议的机制



如果你想从技术上更深入地了解比特币的运作方式，可以参考我们在本工作手册后面提供的相关资源。你也可以在我们的网站上注册比特币文凭——技术版，以便在更多技术课程准备就绪时收到通知。

让我们先来通过一段视频，看看比特币网络是如何工作的。

活动：观看
《比特币的技术原理详解》



正如您在视频中所看到的，比特币网络只是一个分类账或交易记录，存储在多台被称为节点的计算机上。比特币账本是匿名的，这意味着它只有交易和地址信息，而不包含个人信息。账本显示了自 2009 年1月3日网络启动以来，每一个比特币及其变动情况。



第九章

接下来，我们将进一步了解使这一系统成为可能的技术。

9.1 公钥和私钥：通过加密技术实现安全

比特币给我们的是一个硬性承诺：程序将完全按照指定的方式执行。

安德烈亚斯·M. 安东纳普洛斯

9.1.1 公钥/私钥的加密原理

密码学是一种将信息伪装成代码的保密方法。



加密是将信息转换成特殊代码，以致没有正确解密方法的人无法读取的过程。这就类似给保险箱上锁，只有拥有正确钥匙或密码的人才能打开保险箱。

另一方面，解密是将加密信息重新变为可读信息的过程，就像打开保险箱并读取里面的信息一样。

例如，假设约翰想给阿雷尔发送一条秘密信息，且不打算让其他人看到。于是，他们同意在发送前使用猪圈密码加密法来伪装信息，即只有掌握密码的人才能解密信息，其他人无法读取。虽然这种方法在今天看来并不安全，但它实实在在地说明了用私钥加密法发送信息的原理。

如何解密

猪圈密码

在解密猪圈密码时，玩家会得到一个加密消息和一张密码表。要解密消息，玩家就需要在密码表上找到加密消息中的符号，并将其对应到解密的字母。

加密消息示例：

● — —
— — —

A	B	C	J.	K	L	S	W
D	E	F	M.	N	·F	T	U
G	H	I	P	Q	R	V	Z

加密技术在比特币交易中是如何工作的呢？

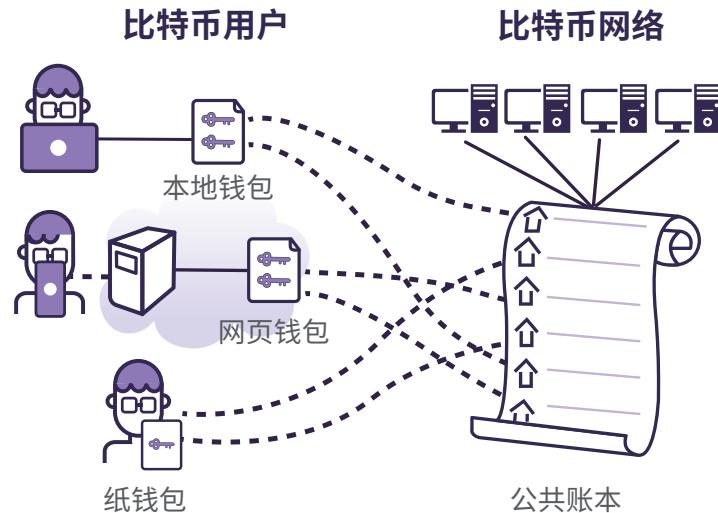
在传统的私钥密码学中，约翰和阿雷尔首先必须共享一个密钥，比如密码或猪圈密码。然后，约翰将使用该密钥加密自己的信息，再将信息发送给阿雷尔。随后，同样知道密钥的阿雷尔将使用相同的密钥解密并读取信息。

但如果其他人掌握了密钥并截获了信息，那么他就可以加密并读取信息。

从技术层面介绍比特币

而在比特币交易中所使用的公钥加密技术解决了这个问题。通过使用公钥加密技术，约翰和阿雷尔不再需要互相分享密码或加密方法。相反，他们各自拥有两把不同的钥匙：一把**公钥**(可以安全地与任何人共享)和一把**私钥**(应该保密)。

在这种情况下，当约翰要向阿雷尔发送信息时，他可以使用阿雷尔的**公开密钥**对自己的信息进行加密，然后再发送给阿雷尔。当阿雷尔收到信息时，只有他能用自己的**私人密钥**解密。其他人即使截获了信息，也无法读取。密钥被窃取的概率也非常低，因为即使是约翰和阿雷尔，也不需要互相分享密钥。



因此，与私钥加密技术相比，公开密钥加密技术的主要优势在于可以在无需发送方和接收方共享密钥(或其他加密方法，如猪圈密码)的情况下实现安全通信，否则可能会被第三方截获。

在比特币中，公钥加密技术并不是用来发送加密信息的，而是被用来创建独一无二的**数字签名**，使比特币交易不可更改。**数字签名**是证明比特币交易真实性的一种方式，在某种程度上类似在实物文件上签名。

公钥加密法 (用于两个用户之间的交易):

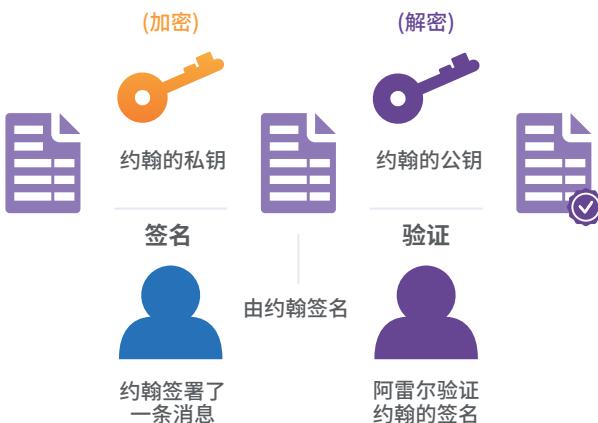
每个用户都有两个密钥，一个是**保密的私人密钥**，另一个是**可与他人共享的公开密钥**。

私人密钥可作为一种身份识别和所有权证明，确认“**此地址属于我，我可以控制它**”。

之所以创建**数字签名**，是为了识别独
一无二的交易。



数字签名





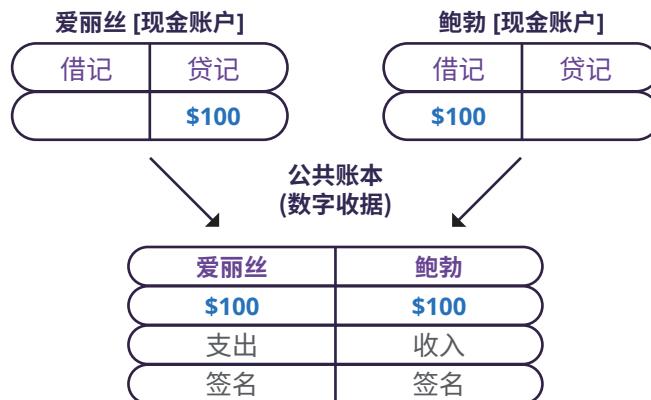
第九章

比特币交易涉及将一定数量的比特币直接转入他人账户。

加密被用来确保只有比特币的真正持有者才能控制并将钱发送给其他人。通过加密，可以确保财产不受恶意行为者的侵害。

作为额外的保护措施，你发送的每一笔比特币交易都会自动获得一个**唯一的签名**。这种**独一无二的签名**由防篡改技术加持，可以帮助网络验证是比特币的真正拥有者发送了比特币，而非其他人。

简单来说，这就是真实比特币交易的原理。



1 创建交易

用户通过指定收件人地址和要发送的比特币金额等详细信息来发起比特币交易。

2 数字签名生成

发送方使用自己的**私人密钥**生成独一无二的**数字签名**。该签名可用于验证交易的真实性，是唯一的加密代码。

3 广播交易

向比特币网络广播已签名的交易，表明发送者有意将比特币所有权转移给接收者。

4 网络验证

比特币在网络上的节点收到交易后，使用收件人的**公开密钥**解密并验证交易的完整性。同时，使用发件人的**公开密钥**验证**数字签名**。

5 在比特币网络上确认

如果验证成功，交易将被添加到分类账中。分类账是对所有交易的安全、透明的记录。一旦确认，比特币的所有权就会正式从发送者转移到接收者。



总之，数字签名由发送者的私人密钥创建，是真实性和所有权的加密证明。数字签名允许比特币的去中心化网络验证交易并将其记录在分类账上。

从技术层面介绍比特币

9.1.2 哈希的解释

请不要被前面的专业术语和数学概念吓倒。虽然并不是每个人都喜欢数学，但即使是最复杂的概念，只要你稍加努力，也能将其掌握。

什么是函数？



函数就像一台机器，能获取一些信息并将其转化为新的东西。你向函数提供的信息被称为输入。函数创建的新信息称为被输出。函数可以帮助计算机完成任务和解决问题。

把它想象成制作沙拉的食谱。菜谱（或函数）会告诉你该使用什么配料以及如何将它们混合在一起从而制作沙拉。你可以放入不同的配料，但配方的输出结果总是沙拉。函数可以让事情变得更容易、更高效。

因此，该食谱是一个将配料作为输入、将拌好的沙拉作为输出的函数。

在比特币中，函数被用来执行交易。我们已经知道，比特币的交易本质上是价值（金钱）从一个地址转移到另一个地址。为了执行交易，需要使用一些加密函数来验证交易并更新比特币分类账的状态。

在比特币交易中使用的函数包括验证交易输入的真实性、检查发送者是否有足够的资金，以及更新相关地址的余额。一旦交易被验证并添加到分类账的区块中，它就会成为网络上所有被永久记录的交易的一部分。



什么是单向函数？

单向函数使用一组指令来处理信息，并将其转化为新的信息，就像冰沙配方将原料转化为新的饮料一样。但就像你不能把冰沙取消混合来换回原来的配料一样，你也不能通过逆转单向函数来换回原来的信息。





第九章



公钥密码学(**公钥**是其中一部分)依赖单向函数的使用，这使得从**公钥**中确定**私钥**变得十分困难。从理论上讲，从**公钥**中找到私钥并非完全“不可能”，但要做到这一点极其困难，而且需要耗费大量的时间和计算能力才能完成这项任务。

在比特币中，从**公钥**中找到**私钥**就像在一个足球场那么大的干草堆中大海捞针。“针”代表**私钥**，“干草堆”则代表所有可能的**私钥**。

同样，单向函数的设计也是不可逆的，无法解密。



什么是哈希函数？

哈希算法就像数字数据的指纹。它是将数字信息转化为固定长度代码的过程，而固定长度代码是唯一的标识符。

就像指纹可以识别一个人一样，哈希值也可以识别数字信息。哈希值在许多应用中都有使用，包括比特币交易。

比特币交易中该如何使用哈希算法

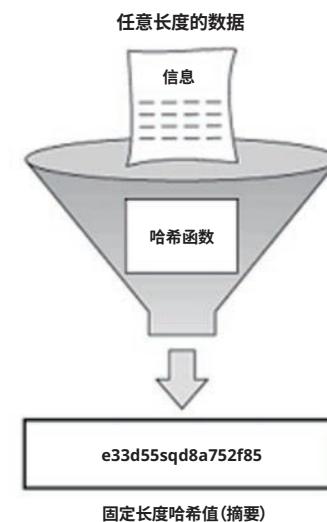
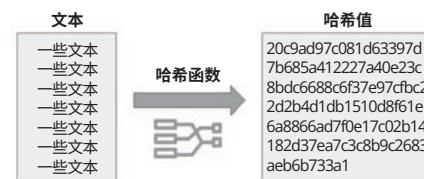
在比特币中，每笔交易在被添加到分类账中的区块之前都要进行哈希算法处理。哈希值作为交易的签名，可用于验证交易是否有效，是否被篡改。如果有人试图更改交易中的哪怕一个字母，哈希值就会完全不同，从而提醒其他人注意。

哈希算法在提供安全方面的作用

哈希值对比特币网络的安全性至关重要。通过使用哈希值来识别交易，网络可以发现任何试图改变或操纵交易的行为。这有助于防止欺诈，并确保所有交易都被准确地记录在分类账上。

散列函数是一种单向函数，它可以接收输入(称为“信息”或“数据”)并将其转换为以数字表示的“哈希值”输出。**输出**的哈希值对**输入**数据是唯一的，因此即使输入数据稍有变化，哈希值也会完全不同。

哈希函数就像一台密码机，可以接收**信息**并将其转化为代码。

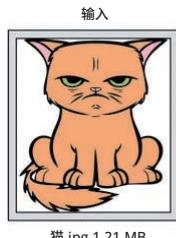


从技术层面介绍比特币

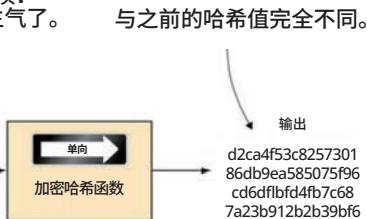
相同的信息，代码看起来也总是一样的。而如果你对信息稍作改动，那么代码就会完全不同。这有助于计算机记忆，并检查其是否有任何改动。



活动 - 生成SHA 256哈希值 →



输出
dee6a5d375827436
ee4b47a930160457
901dce84ff0ffac58
bf79ab0edb479561
一个32字节的哈希值



输出
d2ca4f53c8257301
86db9ea585075f96
cd6df1bfd4fb7c68
7a23b912b2b39bf6
一个32字节的哈希值

无论原始信息有多长，**输出**或哈希值的长度总是相同的。

比特币往往使用几种特定类型的哈希函数，被称为**SHA-256**和**RIPEMD160**。下面举几个例子。

请注意，与第一个输入相比，第二个输入的微小变化会完全改变输出。

第三个输入是一个巨大的文件，但输出仍然与其他两个文件的固定长度相同。

- SHA256 hash of the string **hello world**
- B94d27b9934d3e08a52e52d7da7dabfac484efe37a5380ee9088f7ace2efcde9
- SHA256 hash of the string **hello world.**
- 7ddb227315f423250fc67f3be69c544628dfffe41752af91c50ae0a9c49faeb87
- SHA256 hash of the downloadable iso file **Ubuntu 18.10**
- 7b9f670c749f797a0f7481d619ce8807edac052c97e1a0df3b130c95efae4765

哈希算法也可以看作捕捉音乐精髓的乐谱。就像乐谱是曲调的唯一代表一样，哈希值也是数据的唯一代表。通过比较乐谱和实际演奏，音乐家可以确定演奏是否准确。同样，通过比较接收数据的哈希值和原始哈希值，可以确定数据是否在传输过程中被篡改。





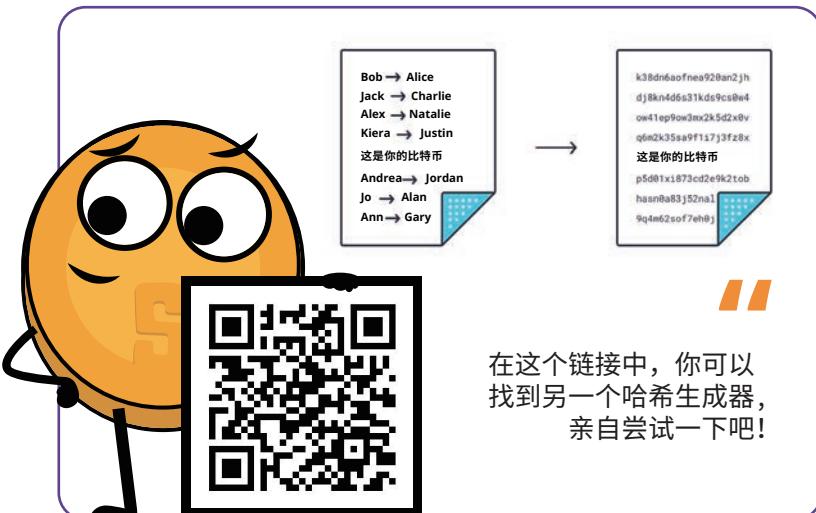
第九章

My
First
Bitcoin

HCM[®]

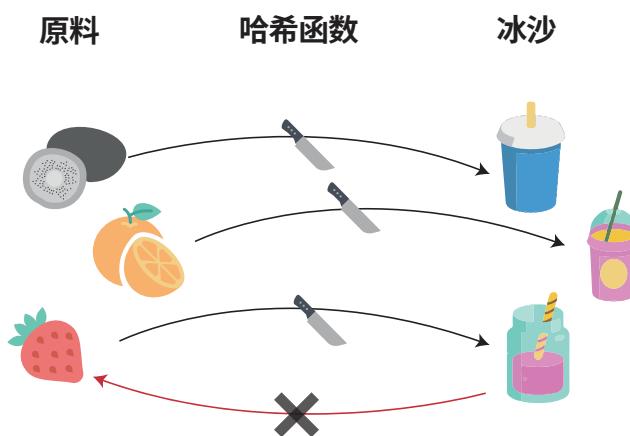
就像音乐演奏中的细微差别会导致声音不同一样，原始数据的细微变化也会导致哈希值的不同。这就使得哈希算法能成为确保比特币交易完整性和真实性的有力工具。

通过哈希算法对**公钥**进行编码的过程，是将信息转换成固定长度、不可读的格式，从而提高信息的安全性。比特币使用 SHA-256 和 Ripemd-160 算法生成公共地址。由此产生的输出作为**公钥**的唯一标识符，有助于确保分类账中存储的交易的完整性和安全性。如果通过这种方式对信息进行加密，那么未经授权的个人就更难访问和篡改数据。



哈希

哈希函数接受任何输入，并生成固定长度的输出(哈希值)。



确定性

相同的原料总是生成相同的冰沙。

原像不可得性

给你一杯冰沙，你无法重新拼凑出一颗草莓。

相关性抗性

稍微改变原料，就会生成完全不同的冰沙。

碰撞抗性

很难找到能生成完全相同的冰沙的不同原料组合。

速度与可验证性

将水果放入搅拌机，快速生成冰沙，并且结果是确定的。

从技术层面介绍比特币

9.2 UTXO模型

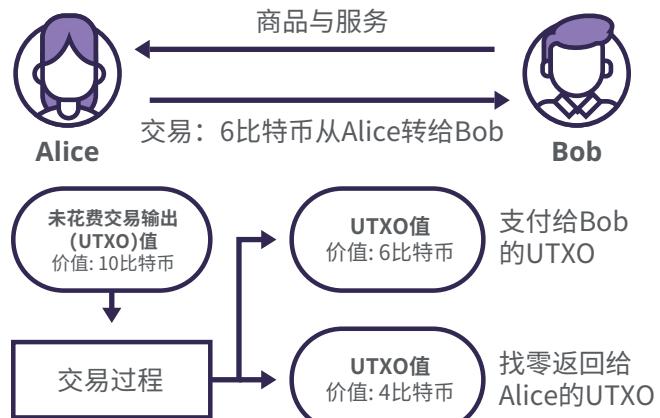
UTXO - 未花费交易输出



什么是UTXOs?

在比特币中，交易就像把一块大金子分成小块，然后再把这些小块发送给其他人和自己。

你可以把UTXO想象成不同大小和块数的比特币，或者钱包里不同面值的纸币。当你花掉一个UTXO时，它会重新生成一个新的UTXO给接收者，剩下的钱则会以另一个新的UTXO的形式寄还给你，这个新的UTXO被称为“零钱UTXO”。这就好比用一张10美元的纸币以6美元的价格买了两杯咖啡。咖啡店保留6美元，并将4美元零钱返还给你。



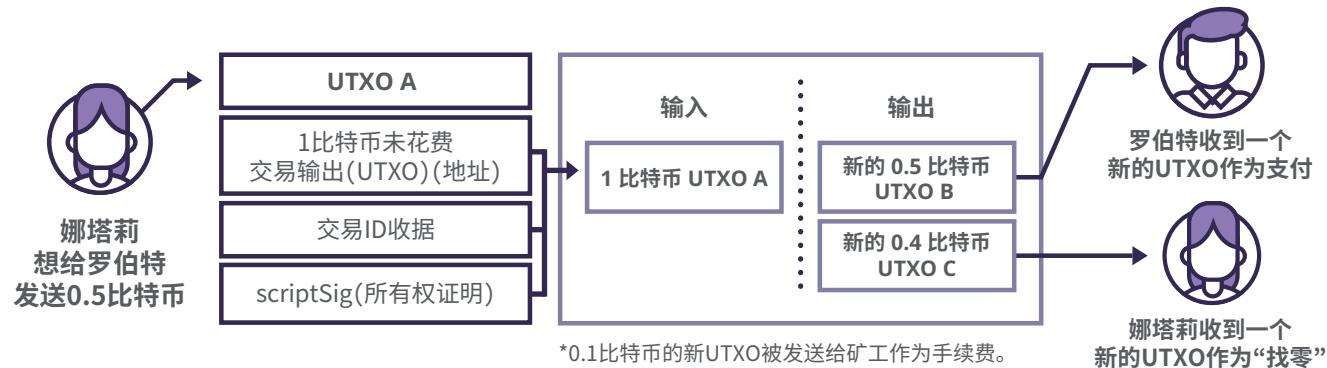
发送比特币时，你总是会发送您比特币钱包中一个(或多个)UTXO的全部金额。那么这样会发生什么呢？你发送一个比特币给收件人，然后你就会收到剩余的比特币，并将其作为零钱存入新比特币地址。你收到的零钱被称为“未用交易输出”或UTXO，可用作未来新交易的输入。

比特币钱包的余额是你所有不同UTXOs的总和。因此，UTXOs的总和就是你所拥有的比特币数量的总和。



需要注意的是，你不应该让别人知道你的UTXO，因为当别人知道你的UTXO时，他们就可以追踪你在网络中的比特币交易，并最终知道你究竟拥有多少钱。

总之，每次进行交易时，你都会使用一个或多个现有的UTXOs来消费比特币，同时也会创建新的UTXOs(对你和收款人而言)。



在进行交易时，被发送的比特币被分成多个输出，每个输出都与一个新的比特币地址(一个新的UTXO)相关联。



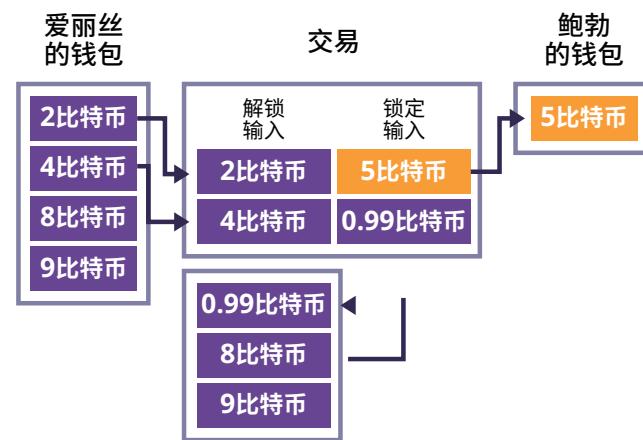
第九章

在向他人发送比特币时，你将使用一个或多个UTXO作为资金来源(输入)。如有必要，这些UTXOs将被合并，以创建属于交易接收者和你自己的新输出。这些新的输出(或UTXOs)将成为收款人和你的财产。然后，这些UTXOs可以在未来的其他交易中被用作资金来源。从第一个区块(2009年1月3日)开始，这个UTXOs链便在比特币分类账上创建了所有比特币交易的透明和可追溯的历史。

举例说明其工作原理：如果你想发送2个比特币，但你只有一个价值5个比特币的UTXO，那么3个比特币的差额将作为“零钱”发回给你。这个零钱对你来说就是一个新的UTXO，你可以在以后的交易中使用这个新的UTXO。

再举一个例子

- 1 爱丽丝想给鲍勃发送5个比特币。
- 2 她从两个UTXO中合并了6个比特币。
- 3 从这些UTXO中，她向鲍勃发送了5个比特币，得到了0.99个比特币作为找零，并需要支付0.01个交易费。
- 4 确认后，交易将被添加到比特币分类账中，更新所有拥有分类账副本的节点。



如果爱丽丝试图用自己已经用掉的一个输出来进行另一笔交易，那么节点会自动拒绝。这是因为节点保存着比特币分类账(及其所有交易)的副本，因此它们可以很容易地检查爱丽丝的UTXOs余额，并确认交易无效。



下面是实际交易的截图，其中只有一个输入。但在另一种情况下，起始余额可能是多个UTXO的总和(多个输入)。观察下面的两笔交易，你能从中发现什么？输入与输出是否一致？你能描述交易的细节吗？两张截图之间有联系吗？先发生的交易是哪个？

从技术层面介绍比特币

9.3 比特币节点和矿工

在本节中，我们将对在第6章中首次介绍的比特币网络的两个非常重要的部分(和参与者)进行更为详细的了解。我们将了解以下内容

1

比特币节点

验证的守门人，其主要工作是保存比特币分类账的副本，从而确保所有交易都是有效的，每个人都在遵守相同的规则。

通过将这项工作分散给世界各地的许多人，比特币能够抵御潜在的问题。这些节点有助于保持系统的可信度，并忠于其去中心化的理念，即没有一个人或团体拥有过多的权力。

2

比特币矿工

即安全的建筑师，他们使用强大的计算机和电力来检查和确认交易，确保一切安全。这项工作有助于使账本或区块链免受任何坏人破坏。

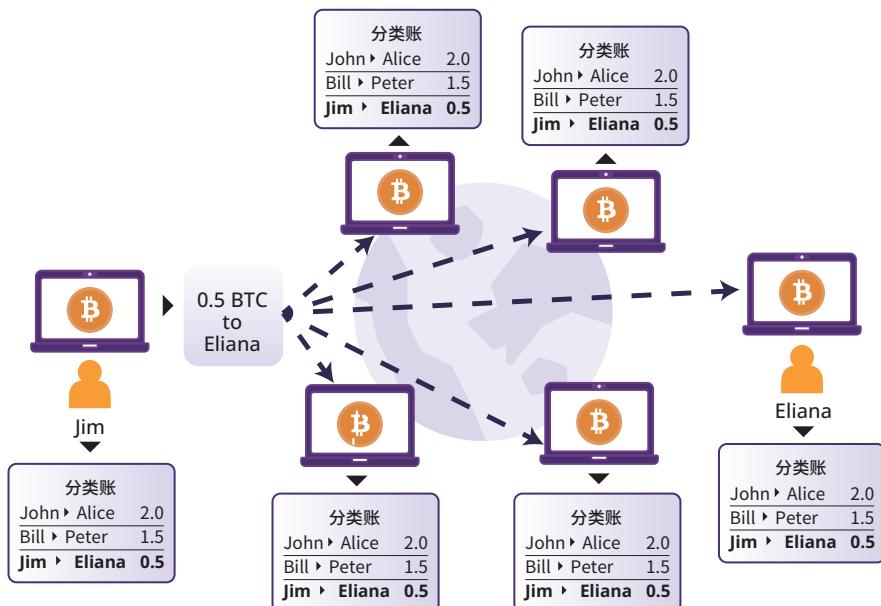
比特币节点和矿工作为一个团队，共同维护着一个去中心化、安全和强大的系统——一种全世界人民都可以依赖的新货币处理方式。让我们更详细地探讨这些角色，了解它们是如何为创新的比特币系统做出贡献的。

9.3.1 什么是比特币节点，我又该如何设置？

比特币节点听起来很专业，但它其实只是一个运行比特币分类账副本的软件。当你运行自己的比特币节点时，你就获得了制定比特币网络规则的发言权。

试想一下：如果有一群人试图改变比特币的运行方式，比如改变比特币的总供应量，而你对比有发言权。那么你可以选择不把你的节点改成新的系统，这就好比通过投票来执行你所支持的网络规则。

让我们把比特币节点想象成一个承担着一些基本任务的数字交通警察。





第九章



验证的守门人

1

比特币节点保存着一份区块链的数字副本，就像所有比特币交易的共享账本。世界各地的许多节点都拥有相同的记录。

通信枢纽

2

节点之间相互连接，形成一个庞大的通信网络。这些节点共享信息，尤其是存储在名为内存池的数字等待室中等待被添加到区块链中的交易。

质量检查器

3

区块链上的每一笔新增交易都要经过严格审查。节点可以确保交易有效，拒绝任何不符合比特币网络规则的交易。

区块链信息提供者

4

其他软件(如钱包)可以向节点询问有关区块链的信息，如比特币余额。节点是信息中心。

新节点欢迎器

5

当一个新节点想要加入时，现有节点会慷慨地提供一份区块链副本。新节点会独立检查每笔交易的有效性，同时强调无信任系统。

活动：
观看关于比特币
节点的视频



运行自己的节点的方法之一是下载比特币核心软件，并给它一些时间下载整个区块链。一旦准备就绪，你就可以将其开启。大约每10分钟就会有新的交易区块到来，而你的节点就会检查它们的有效性，并将它们添加到你本地的区块链副本中。

资源：
比特币核心软件



运行节点为你提供了主权和独立性。你不必依赖他人，运行节点就是你自己的交通警察。与缺乏区块链副本的比特币钱包不同，节点可以确保自给自足。将你的钱包与你的个人节点进行通信，而不是在关于你持有的比特币(以及比特币网络的状态)的事情上信任他人，可以使你的数字体验更安全、更可信。

9.3.2 什么是比特币矿工，挖矿是如何进行的？

“
挖矿的目的并非创造新的比特币。这就是一种激励机制。
挖矿是比特币安全地去中心化的机制。

安德烈亚斯·M. 安东纳普洛斯

从技术层面介绍比特币

矿工收集未经确认的交易，形成一个区块，并耗费能量寻找一个有价值的密钥，以增加并确保该区块在区块链中的位置。



矿工们正在争分夺秒地为区块链添加下一个区块。人们追捧的奖品是“有效区块哈希值”，它被巧妙地隐藏在数十亿个其他区块中，只有网络分配的特定密钥才能将其解锁。

想象一个巨大的干草堆，里面堆满了数以百万计的密钥，每个密钥都代表一个独一无二的区块哈希值。网络选择了一把特定的钥匙来解锁有价值的奖励。矿工们在干草堆中翻找，测试锁中的每一把钥匙，但只有一个幸运的矿工能发现可以完美匹配的钥匙。

一旦矿工找到了正确的区块哈希值，他们就会将其与自己创建的新交易区块一起分享给网络。其他矿工会验证解决方案，以确保其正确无误。如果一切无误，区块就会被添加到区块链中，从而创建一个安全的公共分类账。

矿工可以通过两种方式获得奖励：

- 1 区块奖励**
- 2 交易费**

区块奖励指区块链每增加一个区块，就会有新的比特币进入流通。交易费是用户支付的小额比特币，其目的是让矿工更快、更优先地处理他们的交易。矿工可以选择将哪些交易包含在他们所挖出的区块中，他们通常会优先考虑交易费较高的交易。

比特币减半

比特币减半是比特币宇宙的重要组成部分，有助于长期保持比特币的稀缺性和价值。众所周知，比特币的总供应量为21,000,000枚。这些供应量并不是从比特币推出那天起就完全可用的。相反，这些供应是以循序渐进的方式进入比特币宇宙的。

中本聪巧妙地设计了一个区块奖励系统，可以在没有中央机构的情况下分配新的比特币。在比特币诞生初期，矿工们每挖出一个区块，就能得到50比特币的丰厚奖励，这可以促使他们投资购买功能强大的设备和电力来进行挖矿作业。

为了保持网络稳定和管理新比特币供应，区块奖励大约每21万个区块减半。这一事件被称为“减半”，它减少了进入流通的新比特币数量，同时继续激励矿工保护网络和维护其去中心化。从历史上看，由于进入流通的新比特币供应量减少而产生的减半事件，比特币的市场价格大幅上涨。

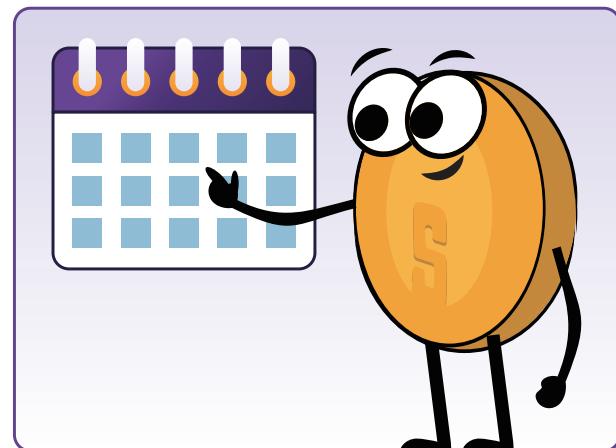


流通供应量指一种货币的总量。对于比特币来说，流通供应总量指在任何特定时间内已经开采出来并在流通的币的数量，其中不包括永远丢失的币。



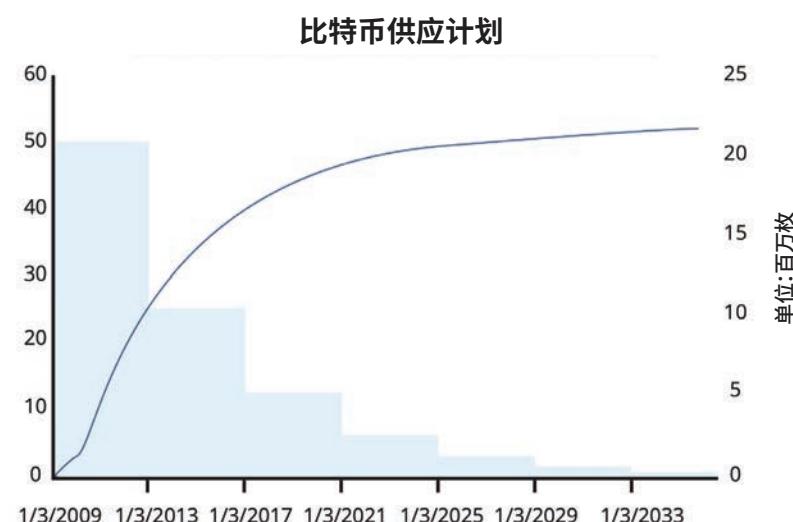
在每次减半事件中，矿工获得的比特币奖励减少，新币的发行率因而降低。因此，比特币的挖矿难度增加，需要维持约10分钟的区块时间，以确保新区块以稳定的速度添加到区块链中。挖矿奖励的减少并不一定意味着矿工的利润减少，因为他们还可以通过验证交易并将其添加到区块链中赚取交易费，这可以抵消挖矿奖励的减少。

比特币协议中预设了减半事件，这使得比特币的供应时间表可预测且透明。



比特币供应时间表是将新比特币释放到流通中的预定和公开计划，旨在长期保持比特币的稀缺性。

下表概述了比特币即将发生的减半事件的细节，包括下一次减半事件的预计日期、发生减半事件的区块编号、减半事件期间的区块奖励(每个挖出的区块)，以及挖出的比特币占总供应量的百分比。



事件	预计年份	区块	区块奖励	挖矿比例
第四次减半	2024	840,000	3.125	96.875 %
第五次减半	2028	1,050,000	1.5625	98.4375 %
第六次减半	2032	1,260,000	0.78125	99.21875 %

从技术层面介绍比特币

随着越来越多的比特币被挖出，流通供应量和已挖出比特币占总供应量的比例将不断增加，直至达到21,000,000枚的总供应量。供应量的减少和需求量的增加会推动比特币价格(以美元计算)上涨。这对早期开采者有利，同时也可以激励矿工继续保护网络安全，为之贡献自己的计算能力和资源。

比特币：已挖出的2100万供应比例

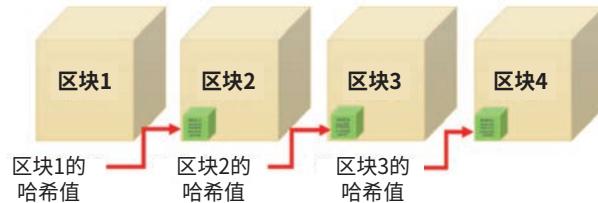


什么是比特币中有效的区块哈希值？

在比特币中，有效的区块哈希值就像矿工试图找到的一个特殊代码。它是一个唯一数字，有助于追踪区块链中的每个区块，而区块链存储了交易信息。从第一个区块（创世区块）到最新的区块，它以链的形式连接在一起，成为所有交易的公开记录。区块哈希值至关重要，因为它将每个区块与之前的区块连接起来，使任何人都能轻松地查看交易历史。区块哈希值有点像每个区块的指纹，可以确保信息的正确性和安全性。区块哈希是确认区块中的数据未被更改的一种途径。



区块通过强制区块之间的特定关系“链接”在一起。也就是说，每个区块必须包含一个“指纹”，即前一区块数据的哈希值。哈希函数可以将任意消息(区块信息)压缩为固定大小(例如160位)，从而生成该消息的指纹。



比特币的创造者中本聪挖出了最初的区块，共计有50个比特币。





第九章



开采区块的竞赛

矿工们通过竞争来发现与网络设定的目标(一个特殊数字)一致的区块哈希值。第一个成功发现正确区块哈希值的矿工有机会将该区块添加到区块链中，并为其分配相应的哈希值ID。这一解决方案可以验证区块的真实性。

可以将挖矿比作一场比赛，其目标是尽快到达终点。找到区块哈希值的难度会定期调整，以确保每个区块在大约10分钟内不断被挖出(随着矿工的加入和离开)。这种机制被称为“难度调整”。

比方说，比特币网络设定的目标数字是1,000。因此，矿工们必须利用他们的计算能力和能量来寻找一个低于1000的区块哈希值(一个特定的数字)。第一个找到低于1000的区块哈希值的矿工可以将新区块添加到区块链中，并获得比特币作为奖励。



比特币挖矿的难度等级是衡量找到符合网络设定目标的有效区块哈希值的难度。比特币挖矿的难度等级每2016个区块调整一次，即大约每两周调整一次，以确保区块以一致的速度被添加到区块链中。其难度级别用数字表示，难度级别越高，找到有效区块哈希值的难度越大。

例如，考虑两个不同的哈希值如下

哈希值1: 0000A1mINgF0RbL0cK5wltHth3hAy5tAcK
难度等级: 1

哈希值2: 00000000A1mINgF0RbL0cK5wltHth3hAy5tAcK
难度等级: 2

在这个例子中，哈希值2的难度高于哈希值1，因为它的哈希值更长，开头的零也更多。矿工更难找到哈希值2，因为他们的计算机需要做更多工作。

通过找到一个有效的区块哈希值，矿工可以证明他们已经完成了将新区块添加到区块链上所需的工作，并获得了比特币奖励和交易费。工作证明(PoW – Proof of Work)是比特币网络用来验证交易和向区块链添加新区块的方法。

从技术层面介绍比特币

PoW 使任何怀有恶意的人都难以控制比特币，因而保证了比特币的安全。

总之，矿工的任务包括以下内容。

1

将交易纳入区块中

当节点验证在“内存池(mempool)”中等待的新创建交易时，矿工会选择其中一个子集，并将其纳入候选区块。

2

工作证明

矿工们相互竞争，以寻找有效的区块哈希值。

3

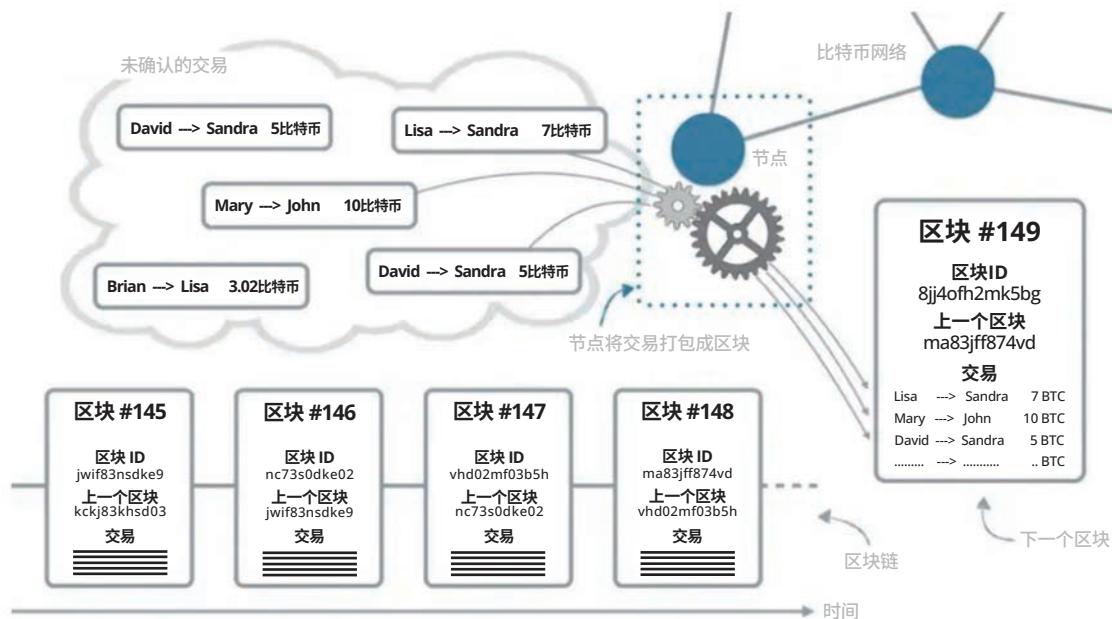
广播有效区块

找到有效的区块哈希后，它们就会向网络传播新区块。

4

赚取奖励

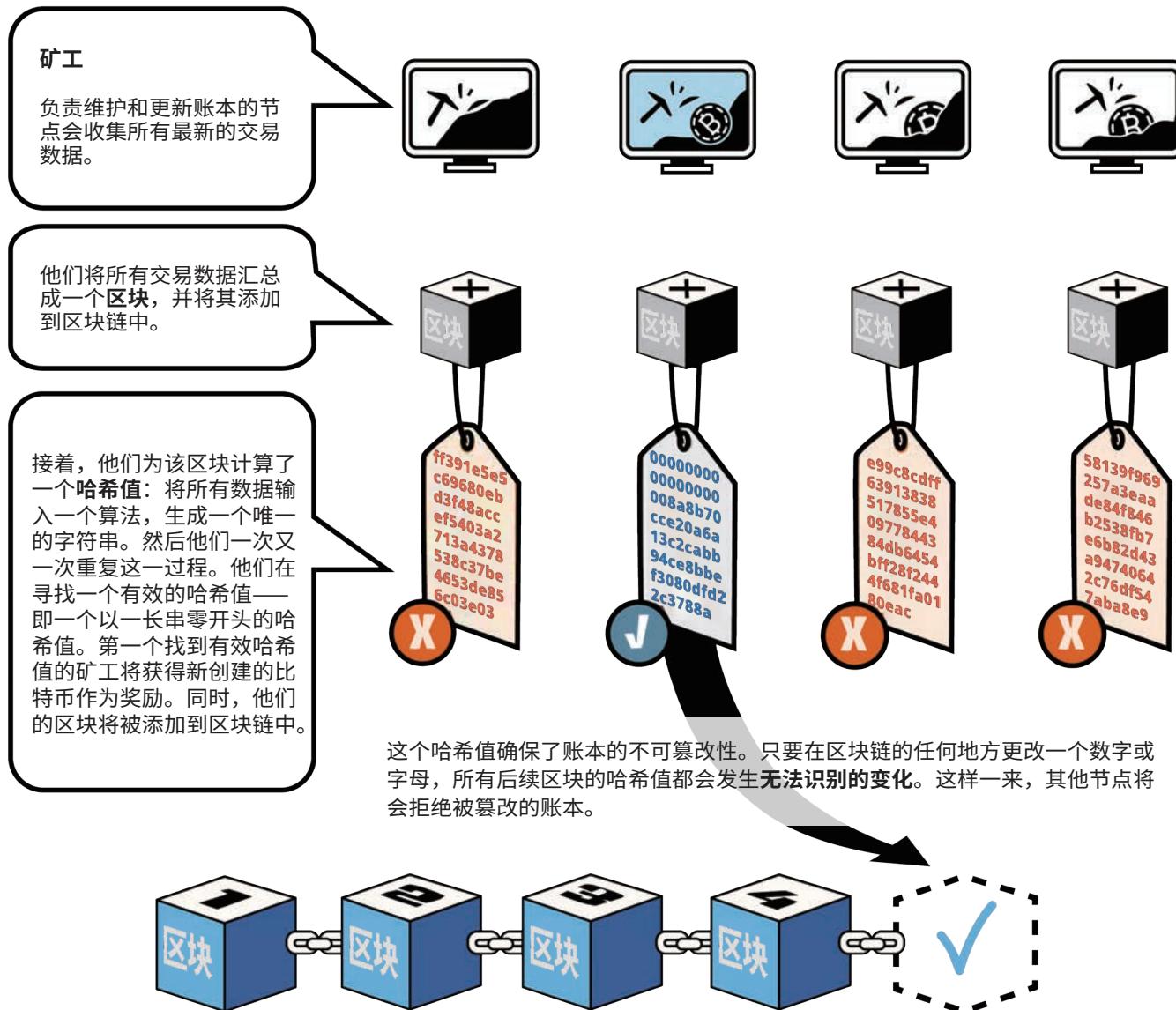
最后，在成功地将区块添加到区块链后，他们会收到新创建的比特币和交易费。



多个矿工可以同时创建新区块。第一个发现符合网络设定目标的区块哈希值的矿工会将其公布给网络，然后其他矿工会检查该矿工候选区块中的交易，以确保其有效。如果交易确实有效，则将该区块添加到区块链中。其他矿工当时创建的其他区块不会被添加，而是会被丢弃。这个过程有助于在网络中保持共识，从而防止重复消费。

候选区块是被考虑添加到区块链中，但尚未添加的一组交易。





9.4 什么是内存池？

“内存池(mempool)”就像比特币网络中交易的等待室。当你在进行一笔交易时，它首先会被广播到内存池，然后才会被验证、选择，并被添加到区块链中。

想象一下，你正在餐厅排队等位。你的名字被添加到等候餐桌的名单中。当有空位时，服务员就会叫到你的名字并安排你落座。比特币在进行交易时同样会被添加到内存池中。当矿工将其加入区块链时，交易就会被确认并添加到区块链中。

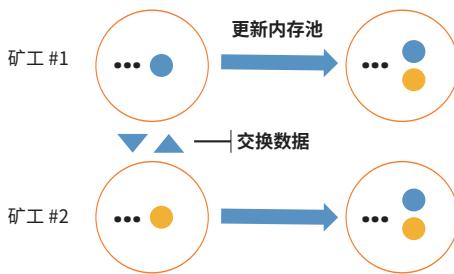
从技术层面介绍比特币



当节点首次从对等节点接收到一笔交易时，需要验证该交易的合法性。毕竟，没有人希望接收错误或具有欺骗性的交易。



内存池同步允许节点通过发送包含内存池中已验证交易列表的消息，并与其他节点共享这些交易。



内存池的主要目的如下。

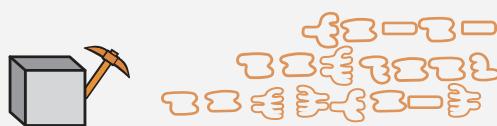
1

传递未确认的交易。



2

为矿工提供可挖矿的交易。



内存池接受 (ATMP) 涉及以下检查事项。

- 我是否已经收到过这笔交易？
- 这笔交易是否与内存池中的其他交易存在冲突？
- 输入的比特币是否覆盖输出的比特币？
- 签名是否证明之前的输出可以使用？
- 手续费是否够用？

如何验证交易并将其添加到内存池？

当新的交易被广播到比特币网络时，节点会对这些交易进行验证，从而确保它们是有效的，并且这些资金在之前没有被使用过。一旦这些交易得到验证，节点将把它们添加到自己的内存池中。然后，节点将与其他节点共享这些交易，以进行双重检查。最后，如果大多数节点都同意，那么这些交易就会被矿工选中并加入区块。不过，如下几个原因可能导致交易在72小时后仍未得到确认。

1 低交易费

费用低的交易可能难以快速处理，因为矿工更倾向于选择费用较高的交易纳入区块。

2 网络拥塞

如果网络拥堵，那么即使交易费用很高，也可能出现延迟确认交易的情况。

3 双重消费尝试

如果恶意行为者试图双重消费，那么其交易可能会被网络拒绝。

4 不正确或不完整的数据

如果交易包含不正确或不完整的数据，那么交易可能会被网络拒绝。

5 交易格式错误

如果格式错误，那么交易可能会被网络拒绝。

为避免交易被拒，建议加入足够高的费用，以确保交易得到及时处理，并在发送之前仔细检查交易中的所有数据是否正确。

活动：内存池

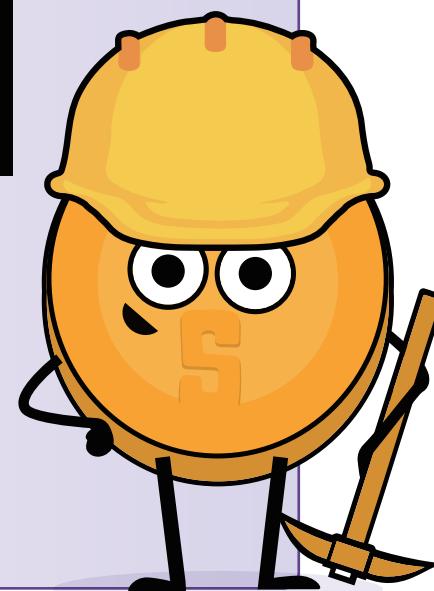
1

扫描以下二维码：

2

查看页面上显示的各种元素，包括最新区块、已确认交易、交易次数、内存使用量和整个区块的近似值。回答如下问题。

- ☀ 上一次开采的区块是什么？
- ☀ 该区块包括多少笔交易？
- ☀ 比特币的交易总额是多少？
- ☀ 区块的大小是多少兆字节？
- ☀ 区块的随机数开头有几个0？
- ☀ 矿工总共赚了多少比特币？
- ☀ 矿工将交易添加到网络中所收到的费用的总值是多少？
- ☀ 选择区块中价值最高的一笔交易。
这笔金额被分到了多少个比特币地址？



从技术层面介绍比特币

9.5 比特币交易如何从开始到完成

1

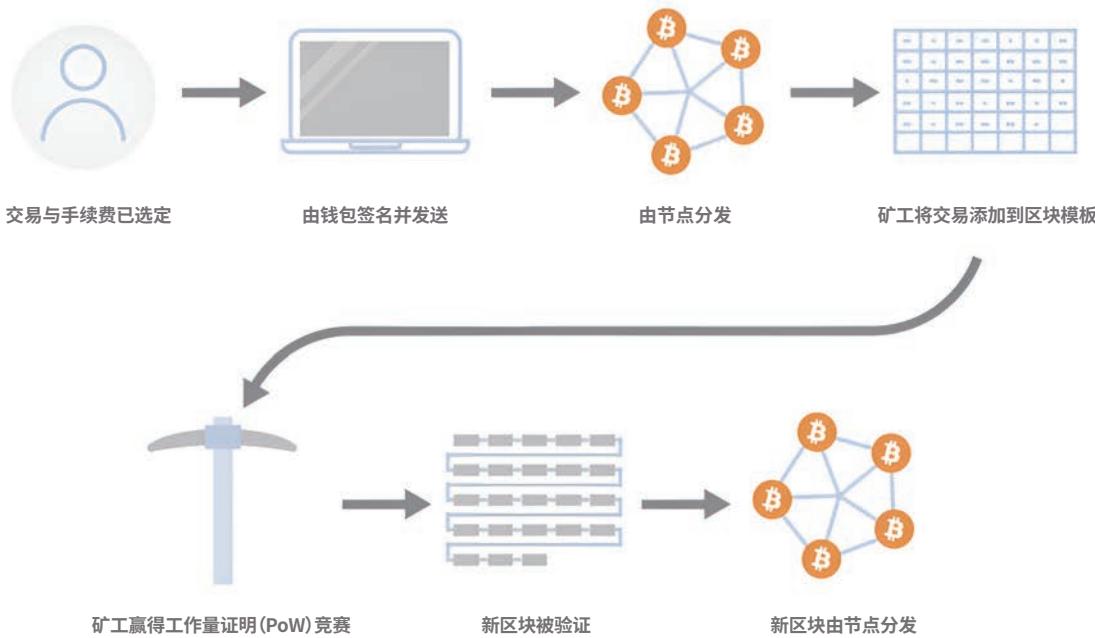
亚当想给格拉多发送比特币。于是他选择了一个UTXO，创建了一个交易，并添加了所有必要的细节，包括他要发送的比特币数量、格拉多的接收地址，以及高于平均水平的交易费用。

2

最后，在检查完所有细节是否正确后，亚当使用自己的私人密钥签署了交易。

3

亚当向比特币网络广播这笔交易。



来源：Stevenot, Ted, “What is a bitcoin node and how does one work?”. Unchained Capital, 2023年1月17日, <https://unchained.com/blog/what-is-a-bitcoin-node/>

4

网络上的节点接收交易，并根据共识规则验证其有效性(如检查亚当的签名是否有效，以及他是否有足够的资金进行交易)。

5

交易被标记为有效，节点会将其传播给网络上的其他节点，并将其添加到内存池中。

6

由于亚当选择了足够高的交易费，所以几乎所有矿工都将他的交易包含在自己的区块中。



第九章



7

工作证明：矿工们争分夺秒地试图通过找到有效的区块哈希值来挖掘自己的区块。其中一个矿工找到了哈希值并向网络广播自己的区块。

8

节点接收新挖出的区块并验证其有效性，这包括验证区块内的所有交易，并确保满足工作量证明要求。

9

大多数节点同意区块有效，并将其添加到区块链中。格拉多在他的接收地址上收到确认的比特币。

10

在随后一小时内，随着更多区块被添加到区块链中，交易的确认次数也在增加。随着交易确认次数的增加，格拉多对交易的成功和不可逆性更有信心。



总结来说：发送者使用其私钥对交易进行签名，节点验证交易中的UTXO(未花费交易输出)，矿工将验证后的交易添加到区块链中。随后接收者可以使用其私钥访问比特币。一旦区块被挖出，那么其中包含的所有交易即可被视为已确认，且在这些交易中作为输入的UTXO被视为已使用，不会被再次使用。

本章结束时，你已经对比特币运作的基本概念有了宝贵的了解。我们已经学习了涵盖从货币基础知识到比特币技术方面的基本内容。现在，让我们在下一章将这一切联系起来吧。在第 10 章，我们将深入探讨一个重要问题：“为什么是比特币？”

第十章

为什么选择比特币？

10.0 引言

活动: 比特币的未来是什么样的？

10.1 什么是中央银行数字货币(CBDCs)，由谁控制？

10.2 比特币的哲学

活动: 课堂讨论：你是否有权控制自己的金钱？

10.3 比特币的优势

10.4 赋权未来

活动: 课堂讨论：你的观点发生了怎样的变化？

为什么选择比特币？

10.0 引言

比特币不仅是一种货币，还是一场将权力归还给人民的革命。
在这个渴望赋权的世界里，比特币让人们尝到了和平与自由的滋味。

我的第一个比特币

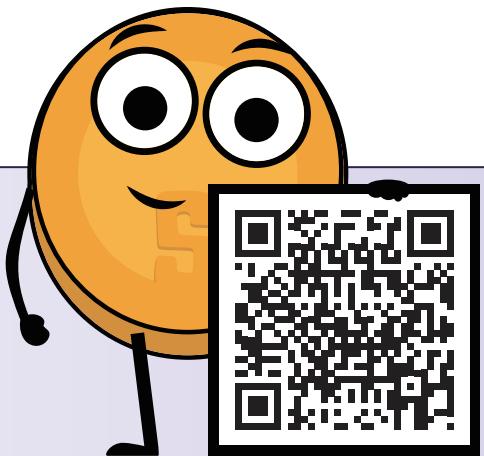
在最后一章中，我们将总结整个旅程中的经验教训，并提出并讨论几个重要问题，共同探讨比特币的未来。

比特币不仅是一种技术，更是一种网络。比特币为一种新的货币形式提供了动力，这种货币的供应量是任何一方都无法改变的。人类从未有过一种供应量固定、没有中央控制的货币形式。如果能得到广泛应用，比特币将成为开启积极变革运动的工具，从而改变全世界人民的生活。比特币代表着一场和平革命，它可以通过创建一个共享的全球货币体系，实现集体自由和公平，并为人类带来新的机遇。

作为一个去中心化的全球系统，比特币实现了更大的金融自由，将权力从少数人手中转移到了多数人手中。它为价值的存储和转移提供了一个安全、抗审查的平台，使个人有能力控制自己的财富、保护自己的购买力。在当今不确定的经济环境下，这一点尤为重要，因为传统金融体系正面临着前所未有的挑战。

活动: 观看视频

积极改变的可能性是巨大的，这就是为什么我们会邀请你通过观看此视频来了解更多信息。



接下来，我们将了解另一种形式的数字货币——中央银行数字货币（CBDCs），并评估它们与比特币的异同。



第十章

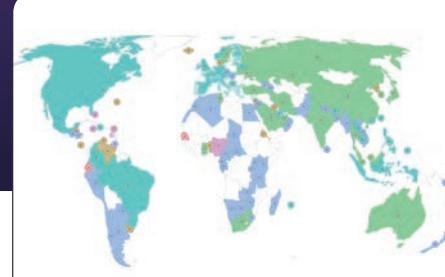


10.1 什么是中央银行数字货币(CBDCs)，由谁控制？

中央银行数字货币或CBDCs是普通法定货币的数字版本。CBDCs遵循与普通法定货币相同的规则，即中央机构(如政府)可以创造更多的供应量，从而降低人们的购买力。然而，CBDCs还为政府提供了新的、强有力的工具，以控制世界各地的人们该如何使用这些货币。

根据人权基金会(HRF)的研究，全球193个政府中有119个正在研究、测试或使用CBDCs。

你可以通过人权基金会的CBDCs追踪器
<https://cbdctracker.hrf.org/home> 或
<https://cbdctracker.org/>

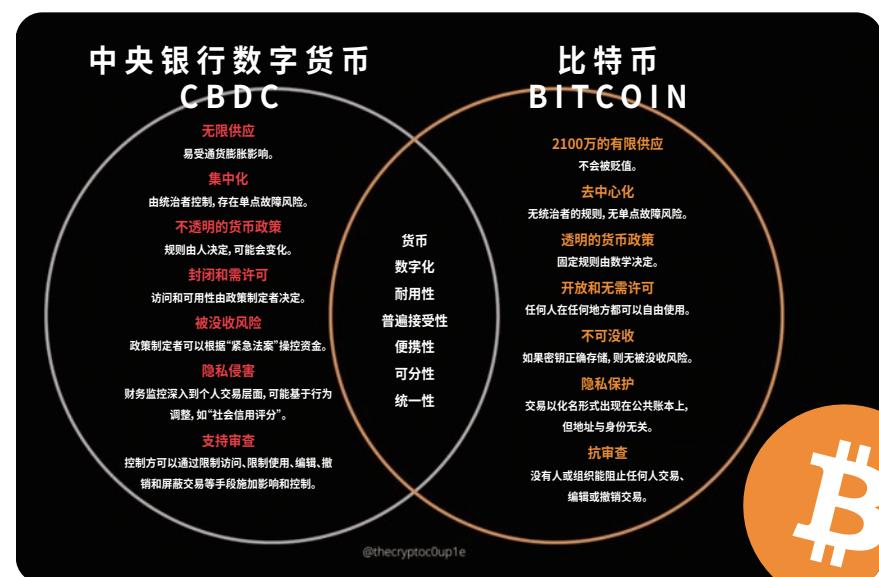


那么除了数字货币之外，CBDCs与普通法币有何不同？
我们必须明白，与纸币或硬币形式的普通法定货币不同，
CBDCs让政府以数字方式监视和控制全球范围内的每一笔
交易。这意味着如果政府不喜欢你或你使用资金的方式，那么他们可以停止某些交易，甚至冻结你的整个账户。

例如，想象一下你想给身处某个需要帮助的国家的家人寄钱，但你所在地的政府拒绝了你的交易，因为他们不同意该国领导人的立场。或者想象一下，你去商店买喜欢的东西，结果因为你社交媒体上表达了自己的观点而不能买。

CBDCs赋予政府无限的权力来控制全球范围内的资金使用，同时限制了个人根据自己的选择花钱的能力。有些人甚至认为，CBDCs可以让强大的政府在全球范围内集中执行专制政策——只需轻轻一按开关，而无需人类执法人员。

CBDCs和比特币都是数字货币，但除了这一共性之外，它们代表着截然不同的货币形式，有着截然不同的理念，并且会给人类带来不同的结果。



为什么选择比特币？

10.2 比特币的哲学

在第6章和第9章中，我们发现运行节点的个人可以帮助维护比特币规则的安全。这是一件大事，因为我们这样的人有史以来第一次可以成为确保货币系统规则得到保护的团队的一员。这些规则包括：货币数量有限，任何一方都不能改变这些规则。对于普通人来说，这是一个帮助我们的货币保持安全可靠的特殊机会。

比特币的理念是关于赋权、自由、财务独立、批判性思维，以及我们都应该对自己选择的系统规则有发言权。与由强大的中央机构控制的法定货币系统不同，比特币是在网络上运行的，没有任何一方可以控制整个系统。这意味着与CBDC等其他类型的货币不同，既没有人可以夺走你的财产，也没有人可以阻止你按照自己的意愿花钱。

在法定货币的世界中，拥有更多的财富直接意味着拥有更多影响力和控制权。与此形成鲜明对比的是，比特币的运作方式是人民掌权。它就像一个团队，其中的每个人无论拥有多少钱，都会在系统中发挥着至关重要的作用。可以把比特币想象成一种集体力量，在这里，你的资金规模并不自动意味着你控制了一切。比特币建立在不可改变的规则之上，在这种和谐的氛围中，就好像是人类自己在控制这个系统——这不是几个大人物在发号施令，而是我们所有人共同努力。这就像一个有韧性的社区，在没有任何单一权威的指点下，指引着比特币的发展方向。

在法定货币体系中，强权主宰着规则。而在比特币生态系统中，是个人的集体力量支撑着网络。任何一个实体，无论其财富多少，都无法左右比特币生态系统的发展。这是对传统权力动态的颠覆——系统的复原力不在少数人手中，而在每个参与者的集体力量中。

比特币的主要理念是创建一个安全、清晰和公平的系统，从而让每个人都能平等地使用全球货币。

活动：课堂讨论——你是否有权控制自己的金钱？

- 1 金钱是人类的必需品和基本权利吗？为什么？
- 2 如果你不能想怎么花就怎么花，不能想寄给谁就寄给谁，也不能带着钱去一个新的国家，那么这些钱真的是你的吗？为什么？
- 3 为什么不再使用易货贸易？需求的双重巧合有什么问题？
- 4 对你影响最大的历史事件是什么？为何理解尼克松冲击及其与每个人的关联在今天至关重要？
- 5 固定供给的货币与传统的法定货币有何不同？



第十章



- 6 比特币是什么时候被创造的，由谁创造，出于什么目的创造，这个目的又是如何定义去中心化系统概念的？
- 7 托管钱包和非托管钱包有什么区别？你最喜欢的钱包是什么？
- 8 你对闪电网络了解多少？你会将它用于哪类交易？
- 9 为什么运行自己的节点可以支持网络？
- 10 在日常生活和未来规划中，我们该如何掌控自己的资金？
- 11 财务自由能在哪些方面提高你为社区或社会做出积极贡献的能力？

10.3 比特币的优势

“超级比特币化”是一种理论上的未来，比特币将成为全球货币体系的主导。这意味着比特币将被每个人、每个地方、每件事所使用——从买咖啡到支付账单，甚至买房子。

个人、企业、国家和政府对比特币的兴趣与日俱增，这凸显了比特币的广泛应用对经济和社会的潜在影响。以下是一个超级比特币化的世界的一些好处。

1 自主权的未来

自主权的未来指全世界的个人都能完全控制自己的数字身份和资产。这将带来更大的金融包容性、自由、隐私和安全，从而促进人类的繁荣、富足和整体幸福。

2 可靠的价值存储

比特币的数字稀缺性使其成为一种可靠的价值储存手段，这可以鼓励更多的人将比特币作为未来储蓄的一种手段。

3 货币政策的变化

如果比特币被广泛采用，就会削弱政府通过传统货币政策工具控制货币供应量的能力。比特币的大规模应用将有可能提高人们的购买力，并鼓励社会转向低时间偏好的活动。

4 增强透明度和可追溯性

区块链上所有交易的防篡改和不可更改记录可提高各行业和部门的透明度和问责制。目前，强大的实体虽然有能力将数万亿美元转移到世界各地，却无法清楚地了解这些资金的去向或使用情况。通过提供公开、可验证的金融交易记录，比特币可以让资本流动变得更加负责任，也使其更容易为公众所了解。

为什么选择比特币？

5 汇款市场的革命

汇款市场涉及资金从一方到另一方的转移，通常是跨越国界的。尽管成本不断下降，但与国内银行转账相比，跨境汇款仍然相对昂贵，尤其是小额汇款。闪电网络可以提供快速、低成本的交易，这使其非常适合汇款市场，并且解决了与汇款相关的高成本和其他挑战，如结算时间慢和营业时间限制等。

6 丰富的能源

当有大量负担得起的能源时，社会就会运转良好，许多行业和社区就能满足家庭、企业和新技术对电力日益增长的需求。比特币挖矿会激励矿工使用多余的能源，这些能源通常会被浪费掉，而这些能源往往来自太阳能、风能和水电等可持续能源。比特币矿工利用这些剩余能源，通过挖矿活动创造新的比特币，以确保网络安全，并在社会需要时将其创造的多余能源回馈给能源网。

10.4 赋权未来

比特币就是货币。

货币帮助人们分辨哪些活动、商品和服务在社会中最重要。正如我们在本课程中所看到的，当货币被中央政府控制时，它就会被操纵。

人类在历史上不断重复的错误之一就是操纵货币，进而对个人、家庭、企业、政府，以及最终的全球人类繁荣造成负面影响。

通过将货币控制权从中央集权机构手中夺走，转而使用任何一方都无法改变的固定供给货币，我们创造了一个不同的世界。在这个世界里，我们不必相信人会做正确的事，而是相信人不会做错事。

这是一个完全不同的世界。

而你，亲爱的学生，你可以参与创造这个世界。使用比特币，运行你自己的节点，帮助你的同胞了解货币的未来——现在，你就是在为一个不同的世界投票。

活动: 最后的课堂讨论——你的观点发生了怎样的变化？

请回答以下 5 个问题。



第十章



我们为什么需要货币？

货币是什么？

为什么选择比特币？

谁在控制货币？

是什么给了货币“价值”？



第十章

 My
First
Bitcoin



你有什么关于货币的问题？把你写下来并和全班同学分享。



回到第1章的第一个活动，将新答案与旧答案进行比较。



比较并讨论原始的答案和问题，和现在相比有什么变化吗？



问自己最后一个问题：我的下一步是什么？我该如何利用这些新知识来增强自己的能力？



如果你已准备好迈出下一步，请查看下一个附加资源部分。在此，我们精选了最佳资源，供你进一步学习和取得成功。

附加资源

1. 为什么使用比特币？

a 《比特币牛市的理由》维杰·博亚帕提:

这篇文章解释了为什么比特币是一种有价值的资产，以及它为什么有潜力成为全球主导货币。作者探讨了比特币在技术和经济方面的优势，使其成为一个强大的投资机会。

b 《比特币的重要性》亚历克斯·斯韦特斯基 (1小时):

本视频讲解了比特币作为一种去中心化数字资产的重要性，以及它是如何影响当前的金融体系的。演讲者探讨了比特币为全球带来金融自由的潜力。

c 《为什么选择比特币》Wiz:

这篇文章概述了使用比特币作为货币和价值储存的好处。这篇文章强调了比特币的去中心化特性，以及它该如何实现更大的金融自由和安全性。

2. 什么是比特币？

a 《比特币技术原理》CuriousInventor:

<https://www.youtube.com/watch?v=Lx9zgZCMqXE> 本视频详细地讲解了比特币的技术原理及其运作方式。

b 《什么是比特币》格雷格·沃克:

这篇文章全面解释了什么是比特币，包括其历史、技术，以及它与传统货币的不同之处。

c 《比特币的起源》RT (30分钟):

该视频探讨了比特币的创立和早期发展过程，揭示了神秘的创造者——中本聪的动机，以及比特币概念的演变。

3. 进一步学习

a 《比特币标准》(1小时40分钟):

这本有声读物探讨了导致比特币诞生的经济和历史背景，介绍了去中心化货币的好处以及比特币成为全球标准的潜力。

b 《奥地利学派与比特币思想》(1小时):

该音频讲座介绍了奥地利经济学派及其与比特币概念的关系，深入探讨了比特币背后的经济原理，以及它在哪些方面与奥地利学派的思想一致。

c 《比特币宝贝》

作者: 娜奥米·万布伊 - <https://bitcoinbabies.com/>
推特: @btcbabies - @ngachanaomi1

一份免费的PDF资源，旨在通过提供涵盖营养、比特币和整体心理健康等重要知识，帮助母亲们获得赋能。

d BTC Sessions

一个专注于比特币教育的YouTube频道，可以提供有用的教程和指南:
<https://www.youtube.com/@BTCSessions>

4. 课程

a 夏季比特币项目

<https://www.summerofbitcoin.org/>:

全球在线夏季实习项目，致力于为大学生介绍比特币开源开发和设计知识。



b Chaincode Labs

[https://learning.chaincode.com/#FOSS:](https://learning.chaincode.com/#FOSS)

提供在线课程和驻留项目，帮助学生学习在比特币协议开发中所需的技能。

c Saylor Academy

提供跨多个学科的免费教育：

<https://www.saylor.org/>

5. 重要作者

- a 亚历克斯·格拉德斯坦: 《检查你的财务特权》
- b 亚历克斯·斯旺:
《接地式相遇疗法: 视角、特点和应用》
- c 阿曼达·卡瓦列里:
《比特币与美国梦: 超越政治分歧的新货币技术》
- d 安妮塔·波什: 《学习比特币: 实现财务主权》
- e 埃里克·耶克斯:
《第七种属性: 比特币与货币革命》

- f 杰夫·布斯:
《明天的价格: 为什么通货紧缩是丰裕未来的关键》
- g 吉米·宋:
《小比特币书: 为什么比特币对你的自由、财务和未来至关重要》
- h 尼克·巴蒂亚:
《分层货币: 从黄金和美元到比特币与央行数字货币》
- i 罗伯特·布里德拉夫:
《感谢上帝有比特币: 货币的创造、腐败与救赎》
- j 琳·阿尔登: 《崩坏的货币》

6. 引用作者

a Curious Inventor:

<https://www.youtube.com/@CuriousInventor>

b 阿尼尔·帕特尔:

推特: @anilsaidso

7. 其他资源

1 Bitcoin.org:

比特币协议的官方网站。

2 Bitcointalk.org:

一个论坛，用户可以在此讨论与比特币相关的话题，提出问题并分享信息，是向比特币专家学习的绝佳场所。

3 Bitcoincore.org:

原始的比特币软件，现在仍被用户和开发者广泛使用，提供强大的工具来与比特币网络互动。

4 Bitcoinwiki.org:

一个社区驱动的资源，可以全面介绍比特币，包括其技术和历史。

5 Bitcoinmagazine.com:

提供比特币和加密货币相关新闻及见解，帮助读者了解比特币的最新动态。

6 Bitcoin.Design:

一个开源资源库，提供与比特币设计相关的图标、模板和网站。

7 NOSTR: <https://nostr.com/>

保护您数据隐私的去中心化社交媒体。

8 Simple X: <https://simplex.chat/>

一个私密、去中心化的通信协议。

9 设置比特币节点:

Keith Mukai的树莓派DIY教程:
https://github.com/kdmukai/raspi4_bitcoin_node_tutorial?tab=readme-ov-file

10 如何选择比特币钱包: <https://bitcoin.org/en/choose-your-wallet>

帮助您选择适合自己的钱包。

11 BitcoinIcons.com: <https://bitcoinicons.com/>

提供免费的比特币图标集合。

12 Bitcoin For Local Business: <https://bitcoinforlocalbusiness.com/>

宣传并与您最喜欢的本地商户分享比特币的价值。

13 Mempool.Space: <https://mempool.space/>

一个开源项目，用以展示闪电网络数据和图表。

各章关键概念

第一章

课程介绍

了解比特币文凭课程的目标和期望。

反思活动 - 定义金钱

参与反思练习，回答有关货币的五个关键问题。

课堂讨论 - 我们为什么需要金钱

参与全班讨论，探讨货币的基本必要性。

分享和比较个人对货币的重要性的看法。

为理解货币在经济体系中的作用奠定基础。

第二章

了解货币

探索货币的基本定义和概念。

讨论班级内的不同观点，把握货币的多面性。

功能、性质和类型

深入了解货币的功能、性质和类型。

认识到这些方面对定义和使用货币的重要性。

货币心理学

了解货币的心理因素，包括稀缺性、时间偏好和权衡。

参与“时间偏好”活动，将心理因素与现实生活场景联系起来。

第三章

货币的历史和演变简介

探索货币的历史和演变，了解古代贸易形式是如何促进我们今天使用的货币的发展的。

货币的演变

探索货币从贝壳和珠子等古代形式，到硬币和纸币出现的转变。跟随从纸币到塑料币的旅程，了解货币在历史上的演变。

数字货币革命

探索当前货币发展的顶峰——数字货币。

了解数字货币是如何仅以电子形式存在，进而在全球范围内实现即时、低成本的交易的。

了解比特币在解决早期数字货币面临的挑战方面发挥的重要作用，使数字货币可以在全球范围内使用。

易货游戏活动

亲身参与易货游戏体验，了解直接交换所面临的挑战，并认识到建立更高效的系统的必要性。

第四章

法币起源

通过简要的历史概述探索法定货币的起源，了解法定货币是如何成为一种主要货币形式的。

部分准备金制度活动

参与部分准备金制度活动，深入了解该系统的运作方式，突出其对债务的依赖以及对更广泛经济的影响。

法币系统

掌握法定货币体系的基本方面，包括其作为法令货币体系的性质、部分准备金银行的作用，以及控制这一体系的主要参与者。

第五章

购买力下降

了解货币通货膨胀的概念及其对购买力的影响。参与通货膨胀的影响：拍卖活动，亲身体验通货膨胀的影响。

全球债务负担与社会不平等

探讨全球债务负担和社会不平等的双重影响。认识个人和社会的后果，强调购买力的丧失和贫富差距的扩大。

法币系统的后果活动

参与“法币体系的后果”活动，揭示当前货币框架的广泛影响。

密码朋克与去中心化

了解密码朋克的故事和他们寻求去中心化货币的动机。区分中心化系统和去中心化系统，从数字货币简史中获得启示。

中央银行数字货币 (CBDCs)

探索中央银行数字货币(CBDCs)不断演变的格局及其对未来货币的潜在影响。

第六章

中本聪和比特币的诞生

探索神秘人物中本聪和比特币的起源故事，了解比特币开发背后的最初动机。

比特币如何运作

了解比特币的机制，包括中本共识机制。识别比特币网络中的主要参与者，如矿工、节点、用户、开发者和项目，并掌握他们之间的协作动态。

课堂活动 - 建立共识

参与“在点对点网络中建立共识”活动，了解该如何在比特币网络中达成共识。

比特币作为健全的数字货币

研究比特币作为健全数字货币的作用，讨论其演变、功能和属性，并参与关于比特币是否符合健全货币条件的全班讨论。

承担个人责任

强调比特币中的个人责任概念，鼓励人们了解个人在去中心化生态系统中的角色和责任。

各章关键概念

第七章

点对点交易

参与去中心化交易，体验比特币交易所的核心原则。

设置比特币钱包

了解下载、创建密钥和备份比特币钱包，从而进行安全交易的基本步骤。

储蓄和DYOR

了解储蓄比特币作为一种价值储存手段，以及独立研究对做出明智决策的重要性。

比特币钱包类型

区分开源、闭源、托管和非托管钱包，了解密钥在安全中的作用。

获取比特币

探索点对点交易和交换等方法，讨论与KYC流程相关的隐私问题。

第八章

闪电网络简介

认识到比特币正通过闪电网络等技术不断发展，其功能不断增强。

设置闪电钱包

了解设置比特币闪电钱包的基本步骤，以促进更快、更可扩展的交易。

体验活动

参与实用的闪电钱包接力赛，促进对闪电网络交易的动态的了解。

闪电钱包类型

针对不同用户的偏好，区分开源、闭源、托管和非托管闪电钱包。

闪电交易

探索发送和接收闪电交易的过程，强调闪电网络的速度和效率。

第九章

比特币账本

了解由节点和矿工推动的去中心化分类账的概念，以确保比特币账本的透明度和安全性。

公钥和私钥

通过公钥和私钥以及演示SHA 256哈希算法的活动，探索加密安全在比特币交易中的意义。

UTXO模型

将未花费交易输出模型作为比特币交易过程的一个基本方面。

比特币节点和矿工

研究节点和矿工在维护比特币网络中的作用，包括发行、稀缺性、减半和难度等。

比特币交易如何运作

深入了解比特币交易的整个生命周期，其中涉及发送方、接收方、节点、矿工和内存池，并有专门针对内存池的活动。

第十章

比特币的理念基础

探索比特币背后的基本理念，了解它是如何作为对经济挑战的一种回应而出现的，重点是比特币对财务自由的影响以及它与传统货币的区别。

比特币的未来

深入探讨比特币作为一种革命性数字货币的潜在轨迹和未来发展。

文凭反思

 总结在比特币文凭课程中的主要收获，鼓励学生反思自己的心路历程以及获得的启示。

 活动包括观看“为什么是比特币？”的视频和重温第1章的问题，从而评估个人理解能力的提高。

术语表

51% 攻击:一种针对区块链网络的攻击，单一实体或群体控制了网络计算能力的多数，从而操控交易甚至可能破坏网络。

山寨币季节:替代加密货币价格显著上涨的时期，通常是由于投资者兴趣和采用率的增加而出现。

山寨币:除比特币外的数字货币。

原子交换:一种点对点的加密货币交换方式，无需中心化交易所或中介。

拍卖:一种以最高出价者为卖出对象的商品或资产交易方式。

以物易物:不使用货币进行商品和服务的交换方式。

商品篮子:用来衡量生活成本变化的一组商品或服务集合。

比特币:一种数字货币或系统，人们无需银行即可相互转账。

区块浏览器:一种用于查看和探索区块链的工具，允许用户查看单个区块、交易和钱包地址。

区块奖励:矿工因在区块链中添加新区块而获得的新比特币数量。

区块链:记录所有比特币交易的公开账本。

BTC:比特币的单位，可以用来购买商品或交易的数字货币。

资本管制:对跨境资金流动的限制。

中央银行 (美联储):政府管理国家货币政策的机构。

中心化:权力或控制集中于单一实体的现象。

中心化系统:权力或控制集中于单一实体的系统。

冷存储:一种将比特币进行离线存储的方法，远离黑客或其他在线威胁。

商品货币:自身有价值并可以作为交换媒介的物品，例如黄金或白银。

确认:网络处理交易的过程，使交易高度不可逆转。“矿工”可以通过其计算机硬件和软件验证交易的真实性。建议等待至少确认六次，以防双重支付。



共识机制: 区块链技术中用于验证交易并确保区块链完整性的方法。

加密货币交易所: 用户可以买卖、交易加密货币与其他资产(如法定货币或其他加密货币)的平台。

加密货币钱包: 一种存储私钥的软件程序，允许用户发送、接收和管理其加密货币。

密码学: 一门有助于创建安全系统的数学分支。

货币贬值: 货币价值通常因硬币中贵金属的含量减少而减少。

债务: 欠他人的钱。

去中心化: 权力和控制分布于网络中，而不是集中于一个中央权威机构。

去中心化自治组织: 由智能合约治理、在区块链上运行，且无需中央管理或结构的组织或网络。

去中心化金融: 加密货币行业中的一种运动，旨在创造运行在区块链上的去中心化金融产品和服务。

去中心化系统: 权力或控制分布于多个实体的系统。

数字资产: 可以交易或作为价值储存的数字化价值表示形式，例如比特币。

分布式账本: 一种分布在计算机网络中，而非存储在一个中心位置的数据库。

双重需求巧合: 在以物易物经济中，两方都恰好拥有对方所需的物品。

双重支付: 一个人试图将其比特币同时发送给两个不同的接收者的行为。

汇率: 一种货币相对另一种货币的价值。

FOMO: 错失恐惧症，用于描述在加密货币市场中因害怕错过获利机会而产生的焦虑或遗憾的情绪。

FUD: 恐惧、不确定性和怀疑，用于描述可能引发市场恐慌或下跌的负面传闻或信息。

GDP (国内生产总值): 一国在一定时期内生产的商品和服务的总价值。

硬分叉: 比特币协议的更改导致区块链的新版本与之前版本不兼容(如比特币现金)。

硬件钱包: 一种用于存储私钥和管理加密货币的物理设备，比软件钱包提供更高的安全性。

哈希函数: 一种数学函数，可以将任意大小的输入数据转化为固定大小的字符串，通常用于加密和区块链技术中。

术语表

哈希率: 测量比特币网络处理能力的一种方式。

HODL: 加密货币社区中的术语，指长期持有加密货币，而不是出售或交易。

热钱包: 一种连接互联网的比特币钱包，允许轻松访问比特币。

进口: 一种经济中商品和服务整体价格水平的上升。

通货膨胀: 发送少量比特币的交易，其金额小到不足以具有经济价值。

首次代币发行: 一种筹资方法，用新加密货币向投资者出售，用以换取更为成熟的加密货币(如比特币)。

第一层协议: 区块链网络的底层，用于处理共识、交易验证和数据存储等基本功能。

第二层协议: 构建在第一层区块链网络之上的次级层，通常可用于提升可扩展性、速度和功能。

账本: 记录财务交易的文件。

闪电网络: 一种第二层支付协议，通过离链通道进行小额交易，从而实现更快、更便宜的比特币交易。

交换媒介: 在商品和服务交换中被广泛接受的对象或系统。

Merkle树: 在比特币区块链中使用的一种树形数据结构，用于高效验证大数据集的完整性。

矿池: 矿工组成的团队，共同工作以提高找到新区块和赚取比特币的概率。

挖矿: 使用计算机硬件为比特币网络进行数学计算的过程，以确认交易并增加安全性。

货币和财政政策: 中央银行和政府分别制定的政策，会影响经济中的货币供应和利率。

货币供应量: 经济中流通的货币总量。

多重签名钱包: 需要多个签名或批准才能执行交易的钱包，可提供额外的安全性和控制权。

多重签名: 一种需要多个私钥授权比特币交易的安全功能。

网络: 一组互连的实体。

节点网络: 支持和维护比特币网络的互联计算机或设备的网络。

节点: 连接比特币网络并参与交易验证和传输的计算机或设备。

不可替代代币:一种数字资产，代表独一无二的物品，通常用于代表艺术品、收藏品或其他独特对象。

随机数:添加到区块头中的一个随机数，用于创建符合难度目标的哈希值。

孤块:因较长的竞争链作废而未被包含在区块链主链中的区块。

纸钱包:用户私钥和公钥的打印副本，用于离线存储和管理加密货币。

点对点:一种去中心化网络，参与者可直接相互交互，而无需通过中央权威。

锚定:一种固定的汇率机制，将一种货币的价值锚定于另一种货币。

私有区块链:由单一组织控制而不是去中心化的区块链。

私钥:一种秘密数据，用以证明某人从特定钱包中花费比特币的权利，可通过加密签名实现。

权益证明:一种共识机制，要求用户持有一定数量的加密货币才能参与交易验证。

工作量证明:一种共识机制，要求用户完成一定量的计算工作以参与网络。

公有区块链:任何人都可以参与并验证交易的区块链，可以使其实现去中心化。

公钥:通过数学过程从用户的私钥派生的唯一标识符，用于接收比特币。

公钥/比特币地址:用于接收比特币的公开密码或号码。

公共账本:一个去中心化的数据库，记录比特币网络中所有交易的公共记录。

购买力:用货币购买商品和服务的能力。

恢复短语/种子关键词:

一系列12、18或24个单词，可用于生成多对私钥和公钥，并用于恢复比特币钱包。

准备金率:银行必须保留作为准备金的存款比例。

限制性银行:对银行服务或访问银行服务的限制或约束。

中本聪:比特币匿名创始人(或创始团队)使用的化名。

聪(sat):比特币的最小单位，相当于 $1/100,000,000$ 比特币，以比特币的创造者中本聪命名。

术语表

每字节的聪: 用于衡量比特币交易费用的按每字节支付的聪的数量的单位。

隔离见证: 一种比特币协议升级，可改变数据在区块链上的存储方式，从而增加容量并降低交易费用。

侧链: 一个连接到另一个区块链的区块链，允许在两条链之间转移资产或信息。

签名: 一种用于证明所有权的数学机制。

智能合约: 一种自动执行的合约，合同条款以代码的形式写入。

软分叉: 一种比特币协议的更改，向后兼容旧版本软件。

稳定币: 一种加密货币，通过锚定法定货币或其他资产来维持稳定价值。

供需: 一种经济原理，商品或服务的价格由供给量和需求量的相互作用决定。

货币的时间价值: 货币在当下的价值高于未来的价值的原则。

代币: 在区块链上创建的价值单位，通常用于表示特定生态系统中的资产或功能。

代币化: 在区块链上创建资产或资产类别的数字表示的过程，用以实现部分所有权和可转让性。

交易对: 一组可以在加密货币交易所中相互交易的货币或资产。

交易费用: 发送方支付的一小部分比特币，用于激励矿工将交易包含到区块中并添加到区块链。

交易ID: 一串数字和字母，用以显示比特币转账的详细信息(如转账金额、发送方和接收方地址，以及转账日期)。

交易: 在比特币网络上从一个地址向另一个地址转移比特币的过程。

无信任系统: 一种不依赖于任何第三方或中介，而是依靠基础技术的安全性和透明度的系统或交易。

双因素认证: 一种安全措施，要求使用两种身份验证方式(通常是密码和单独的代码或设备)来访问账户或完成交易。

无银行账户: 没有传统银行服务访问权限的个人或社区。

记账单位: 用于表达商品和服务价值的标准计量单位。

波动性: 资产价格随时间而波动的程度。

钱包地址: 用于在比特币网络上发送和接收比特币的唯一标识符，通常由一串字母和数字组成。

钱包备份: 比特币钱包的私钥和恢复短语/助记词的副本，可在原件丢失或被盗时用于恢复钱包的访问权限。

钱包: 一个虚拟容器，用于存储比特币，类似物理钱包，包含允许你花费分配在区块链中的比特币的私钥。

鲸鱼: 持有大量加密货币的个人或组织，能够通过大规模交易影响市场价格。

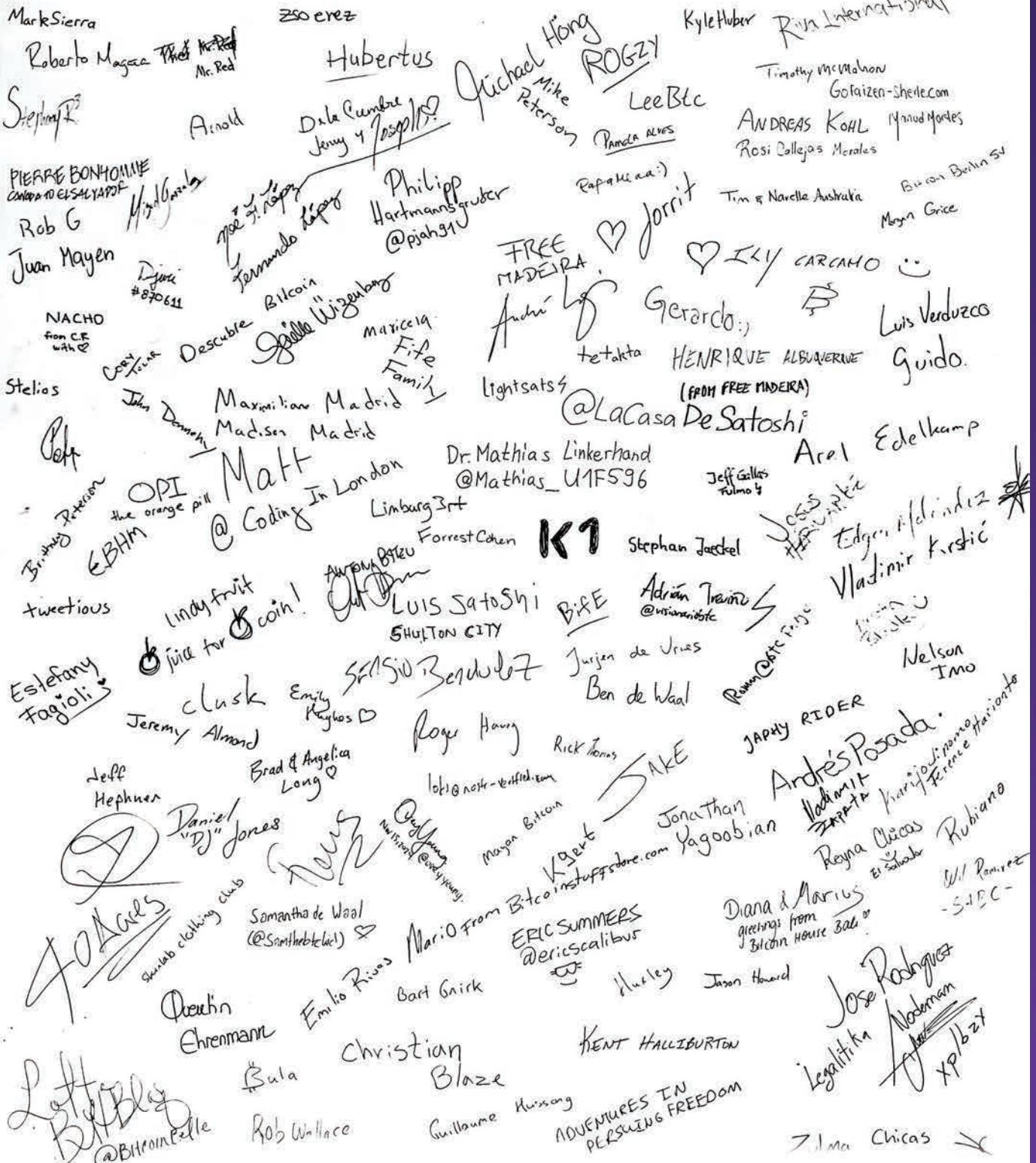
白帽黑客: 可以使用其技能来识别和修复计算机系统和网络漏洞的道德黑客。

白皮书: 一份解释区块链项目或加密货币试图解决的问题及其解决方案的报告。

XBT 和 BTC: 比特币的缩写。

因你而独立!

感谢所有在 Geyser 活动或
Adopting Bitcoin 2024 期间
支持我们的捐赠者!



感谢大家!



EL SALVADOR



中文版 | 2025